INTECO

Instituto Nacional
de Tecnologías
de la Comunicación

Estudio sobre usuarios y entidades públicas y privadas afectadas por la práctica fraudulenta conocida como *phishing*

Octubre 2007

OBSERVATORIO DE LA SEGURIDAD DE LA INFORMACIÓN

ÍNDICE

PUNTOS CLAVE

I La utilización ilícita de Internet

- No se puede considerar que las redes de comunicación, y en particular Internet, constituyan un foco de nuevos delitos, muchas veces, simplemente, son foco de nuevas versiones de prácticas ilegales preexistentes.

  Al igual que en el delito tradicional, el fraude a través de Internet se caracteriza por su constante evolución. El fraude electrónico continúa desarrollándose y ganando en sofisticación; pero, paralelamente, los usuarios (domésticos, empresas y administraciones) al igual que en el mundo físico, resultan menos vulnerables gracias a mejores hábitos de utilización de la Red y a una mayor protección de los equipos.

- El delito informático produce un impacto económico negativo: no solo el daño directo para el que sufre o asume la estafa, sino también las pérdidas derivadas de la erosión de la imagen del suplantado; ambas provocan un impacto social, que se traduce en un freno al desarrollo de la Sociedad de la Información.

- **El *spam* o** mensajes **de correo electrónico no solicitados** que son enviados en cantidades masivas a un número muy amplio de usuarios **suponen, en muchos casos, la cabeza de puente para la comisión de un fraude electrónico** (*phishing*, *scam,* "cartas nigerianas", bulos, etc.).

- Una primera clasificación distinguiría entre los **delitos que tienen su origen en técnicas de ingeniería social y los que tratan de aprovecharse de vulnerabilidades de los sistemas.** No obstante, en algunos ciberdelitos se combinan ambos orígenes.

  Siguiendo el Código Penal español de 1995, se distingue entre los supuestos basados en técnicas de ingeniería social, que son tipificados en el mismo apartado que las estafas tradicionales (Art. 248.1 Código Penal), y los supuestos de utilización de código malicioso (*malware*) o de intrusión en sistemas de información recogidos en el artículo 248.2 del CP.

  Dentro del primer grupo se encuentran algunas de las **estafas tradicionales "puestas al día" para el mundo Internet.** Forman parte del segundo grupo aquellos fraudes que utilizan códigos maliciosos o métodos de intromisión ilegal en los sistemas de información, por lo que es normalmente necesaria, una mayor habilidad técnica por parte del ciberdelincuente.

II Resultados cuantitativos de la investigación: estadísticas sobre el fraude a través de Internet para los usuarios españoles

- **Es importante señalar que los datos de los resultados cuantitativos que se muestran a continuación tienen su base en opiniones y percepciones de los usuarios encuestados.**

- El término *phishing* es conocido por un 41,2% de los usuarios de Internet españoles, otros tipos de fraude son menos conocidos.

- **El 29,9% de los usuarios reconocen haber sufrido algún intento de fraude online**, aunque **sólo afirman haber sufrido un perjuicio económico el 2,1%** de los usuarios españoles de Internet.

- **La media de perjuicio económico se sitúa en 593€,** si bien en más de **dos de cada tres casos no supera los 400€** que es el límite establecido en el ordenamiento jurídico español para que tenga la consideración de delito.

  El 24,8% de los ataques no alcanza los 50€. Este hecho contribuye a que, en muchas ocasiones, los fraudes no sean detectados al camuflarse entre los apuntes bancarios corrientes.

- Un 80,2%, de aquellos usuarios de Internet que han sido objeto de un intento de fraude **no modifican sus hábitos** de utilización del servicio de banca online, y un 73,1% no modifican sus hábitos de comercio electrónico.

- Incluso cuando dicho intento conlleva un **perjuicio económico**, no se produce un abandono masivo de los servicios de banca ni compra online: no alteran su comportamiento un 52,4% y un 31,9% respectivamente. Este hecho es debido a una doble motivación: por una parte, no se culpabiliza a las entidades financieras y empresas de dicha estafa (incluso el grado de e-confianza en la banca apenas se resiente); y, por otra parte, las ventajas de dichos servicios se valoran mucho más que los posibles problemas

III Posicionamiento y papel de los agentes afectados por el fenómeno del *phishing*

El Estudio identifica el posicionamiento y papel de los agentes afectados y a la vez intervinientes en el ámbito de desarrollo del fenómeno del phishing, describiendo las medidas de actuación concretas y activas que cada uno de ellos, bien de forma individual o en conjunto, desempeñan a lo largo del proceso:

- El **sector bancario** en España está adoptando un comportamiento ejemplar: una vez saben que un cliente ha sufrido una estafa en su cuenta a través de Internet, están

asumiendo el coste que conlleva el daño producido. El interés de las entidades financieras es doble y recae, de un lado, en que sus clientes conozcan y tomen las medidas de seguridad más oportunas para evitar que se produzca cualquier tipo de fraude a través de la Red y, de otro, en lo que respecta a la propia Entidad, con el objeto de activar todos los mecanismos de seguridad necesarios para prevenirlo.

- Como principales afectados por los fraudes a través de la Red, en general, y por el *phishing* en particular están liderando, entre otras, las siguientes medidas de prevención:

  - La contratación de servicios de empresas de seguridad.

  - El desarrollo de su propio departamento interno de seguridad de la información.

  - Y, el fortalecimiento del Grupo de Trabajo de Seguridad Informática del Centro de Cooperación Interbancaria (CCI) que trabaja en la coordinación de las entidades financieras, la puesta a disposición de información y la promoción de iniciativas para sugerir iniciativas a la Administración Pública: la implementación de un sistema que dificulte el registro de marcas similares a otras reconocidas, la promoción de reformas en el Procedimiento de Cancelación de dominios, la habilitación de mecanismos de aviso a las entidades o el establecimiento de un procedimiento ágil que facilite solicitar el bloqueo de cualquier dominio ".es" utilizado para fines fraudulentos.

- La principal labor de los **fabricantes y proveedores de servicios de seguridad informática** consiste en ofrecer productos y prestar servicios de soporte a las empresas, usuarios y administración para mejorar su seguridad. Trabajan principalmente en dos frentes: la prevención del fraude (desarrollan parches de seguridad minimizando las posibles vulnerabilidades de los sistemas operativos y programas informáticos y prestan servicios a las propias entidades financieras con sistemas de filtrado del tráfico, de protección ante intrusiones, detección de webs fraudulentas, etc.) y la investigación e innovación tecnológica colaborando con otros agentes implicados como son los Cuerpos y Fuerzas de Seguridad del Estado.

- El **Poder Judicial y los Cuerpos y Fuerzas de Seguridad del Estado (CFSE)** tienen un papel crucial en el proceso del fraude online, realizando la labor de vigilancia y persecución de las estafas informáticas. En ambos casos, se han creado grupos especializados con personal altamente cualificado y experimentado en este tipo de delitos informáticos desempeñando labores de carácter reactivo (investigación de la procedencia del fraude y persecución y reprensión del autor) y proactivo (tareas preventivas y de vigilancia consistentes en el rastreo de la Red en busca de sitios webs de carácter fraudulento que se encuentren activos). Se ocupan de la

tramitación, instrucción y enjuiciamiento de las denuncias recibidas directamente por las propias entidades financieras o a través de sus clientes. Asimismo, las empresas de seguridad informática y los organismos como INTECO (a través de su CERT[1]) también les aportan información de gran valor para la persecución del fraude.

- El compromiso de las **Administraciones Públicas** con los sistemas de seguridad informática es claro. Las actuaciones puestas en marcha abarcan todos los niveles y fases del proceso: desde la creación de diferentes métodos de prevención y disuasión, pasando por la participación en la reducción de los efectos, y la persecución de las conductas delictivas que afecten a la seguridad de los sistemas de información. Se han puesto en marcha:

  - Medidas de carácter normativo destinadas principalmente a ejercer un efecto disuasorio entre los potenciales autores de este tipo de fraudes. Así se han llevado a cabo medidas de carácter legislativo: la Ley de Servicios de la Sociedad de la Información y el Comercio Electrónico, la L. O. de Protección de Datos así como modificaciones en el Código Penal destinadas principalmente a ejercer un efecto disuasorio entre los potenciales autores de este tipo de fraudes.

    Además se han puesto en marcha diferentes iniciativas, dentro de la promoción general de la Sociedad de la Información, con un carácter mixto, tanto de divulgación y difusión, como de potenciación legislativa entre los países miembros. Así, en el ámbito europeo, la Comisión Europea determinó en 2004 la creación de ENISA, la Agencia Europea de Seguridad de las Redes y de la Información (www.enisa.europa.eu) y en mayo de 2006 plantea una estrategia basada en el diálogo, la asociación y la potenciación para afrontar algunos de los principales retos de seguridad que se plantean, como el incremento de comunicaciones con dispositivos móviles, el aumento de los ataques y, especialmente relevante a este efecto, la sensibilización de la opinión pública.

  - Medidas de prevención y refuerzo de la e-confianza en las que el DNI electrónico se configura como uno de los programas más ambiciosos puestos en marcha por la Administración, que se posiciona como una herramienta fundamental para la lucha contra estas amenazas: el fraude electrónico, la propagación del código malicioso, la suplantación de identidad o la ingeniería social.

  - Medidas relativas al estudio, formación y divulgación con el objeto de: a) ofrecer información rigurosa y transparente a la opinión pública, b) promocionar

[1] Centro de Respuesta a Incidentes en Tecnologías de la Información para Pymes y Ciudadanos

acciones de formación para ciudadanos y empresas sobre buenas prácticas y hábitos de seguridad de la información, y c) establecer mecanismos de prevención y defensa, para que los usuarios finales utilicen y se beneficien de modo seguro y confiado de cualquier servicio o facilidad relacionado con las TIC y resulten menos vulnerables ante un posible delito de esta naturaleza.

- Las **Asociaciones de Usuarios y Consumidores** desempeñan acciones para proteger al usuario final de Internet entre las que destacan: el rastreo de la Red para localizar páginas web fraudulentas, la realización de campañas de comunicación, la colaboración con los diferentes agentes implicados en la seguridad online, etc.

- El comportamiento prudente y responsable de los **usuarios** finales en la navegación unido a la utilización de medidas y herramientas de seguridad informática que pueden encontrar actualmente en el mercado, merma la capacidad de éxito de los ciberdelincuentes.

IV Resultados cualitativos de la investigación: propuestas y recomendaciones de los propios agentes afectados por el *phishing*

Los diferentes perfiles de expertos consultados durante la investigación cualitativa – entidades financieras, empresas prestadoras de servicios a través de Internet, medios de pago, fabricantes y proveedores de soluciones de seguridad, Administración Pública, Fuerzas y Cuerpos de Seguridad del Estado, abogados, juristas y expertos en Derecho, y asociaciones de consumidores y usuarios – proponen una serie de recomendaciones a los diferentes agentes intervinientes en el proceso:

- **Dirigidas a las entidades financieras y empresas prestadoras de servicios de Internet**:

  - ***Bancos, cajas de ahorros y cooperativas de crédito***: la propuesta de ***recomendaciones*** generales dirigidas por los expertos a este colectivo va dirigida a aunar esfuerzos en la lucha contra este fraude mediante la colaboración internacional con empresas del sector de la seguridad informática, operadoras de telecomunicaciones, gestores de nombres de dominio como Red.es o la ICANN[2], las Fuerzas y Cuerpos de Seguridad del Estado y los Equipos de Respuesta a Emergencias Informáticas[3] gubernamentales (como el IRIS-CERT, el CCN-CERT o el INTECO-CERT). Como recomendaciones de carácter avanzado merecen especial atención: la utilización de sistemas de autenticación fuerte (tarjetas de coordenadas y token de seguridad), la

[2] Internet Corporation for Assigned Names and Numbers

[3] CERTs: Computer Emergency Response Team – Equipos de Respuesta a Emergencias Informáticas) dependientes de los diferentes gobiernos de todo el mundo.

aplicación del modelo de negocio de las tarjetas de crédito, la implementación de reglas lógicas y de comportamiento[4], la instauración de avisos a móviles mediante mensajes cortos (sms), etc.

- ***Empresas prestadoras de servicios a través de Internet***: los expertos proponen incidir en la seguridad como aspecto crítico para el negocio así como considerar los recursos destinados a proteger la seguridad de los sistemas de ***información*** como una inversión. La propuesta de recomendaciones avanzadas distingue entre recomendaciones de carácter técnico (la obligación de solicitar el código CVV2[5], sistemas inteligentes de prevención del fraude, filtrado del tráfico, etc.) y de carácter organizacional (establecimiento de un Plan de Seguridad de la información, de Políticas de Prevención, un Plan de Formación y de Recuperación).

- **Dirigidas a los fabricantes y proveedores de servicios de seguridad informática.**

  - *La certificación del software*. Es recomendable que los productos que llegan a los usuarios cuenten con una certificación de seguridad, con esquemas que obliguen a los fabricantes a contrastar dichos productos y verificar su calidad. Todo el software utilizado por los ciudadanos debe haber sido sometido previamente a pruebas capaces de avalar su seguridad por laboratorios independientes acreditados.

  - *El desarrollo de estándares de seguridad*. Una segunda recomendación consiste en el desarrollo de unos estándares de seguridad, para poder validar y contrastar los certificados digitales por parte de laboratorios especialistas en protección de datos. De esta forma, se podría homogeneizar todas las certificaciones digitales que existen en el mercado, para establecer un protocolo de seguridad común.

  - *Mejorar las actuaciones por parte de los operadores para realizar un bloqueo de determinados servicios*, como puede ser el bloqueo del correo de salida que puede ser fácilmente monitorizable a través de un filtro que controle el tráfico del puerto 25, para aquellas máquinas cuya IP se identifique asociada a un uso malicioso del servicio de correo, distribuyendo *spam*, *malware* y troyanos, o un control en el acceso a aquellas máquinas que alojan sitios fraudulentos.

[4] Reglas basadas en la memorización de las pautas de conducta del usuario, permitiendo establecer alarmas de riesgo ante posibles casos de fraude. Se trata de un sistema de protección que tiene un reducido coste, tanto económico como de funcionamiento, de las que el sector de las entidades de medios de pago cuenta con una sólida experiencia.

[5] El código CVV2 (Card Verification Value) es un código de seguridad elaborado por las compañías de las tarjetas de crédito (Visa, MasterCard y American Express). Con este mecanismo de autenticación se identifica la posesión de la tarjeta empleada para el pago en las transacciones realizadas a través de la Red.

- *Aplicación de políticas avanzadas de gestión de correo electrónico* proporcionando por ejemplo un servicio de salida de correo electrónico cortado por defecto, obligando a que el envío de ese correo se valide por el servidor del proveedor (ISP), donde se puede instaurar un mayor control del flujo de comunicaciones con restricciones y medidas de seguridad contra el mal uso del correo electrónico y que, de esta forma, pueden resultar transparentes al usuario.

- **Dirigidas al Poder Judicial y los Cuerpos y Fuerzas de Seguridad del Estado**: se orientan a la optimización operativa en la lucha contra el fraude por lo que se recomienda favorecer y estimular de forma activa la formación continua de jueces y fiscales sobre este tipo de delitos a través de la Escuela Judicial y el Centro de Estudios Jurídicos. Por otro lado es necesario formar a jueces y fuerzas de seguridad en un lenguaje común. Se hace especial hincapié en la cooperación policial y coordinación entre los distintos CFSE y, de especial manera, con los jueces y tribunales así como con otros organismos de la Administración competentes en la materia. Para facilitar la persecución de este tipo de fraude, se propone que se instaure una Fiscalía y juzgados especiales para la instrucción de delitos informáticos.

- **Dirigidas a las Administraciones públicas:** En su papel de tutelaje de los sistemas de información y comunicación a través de los distintos organismos públicos competentes (Jueces y Tribunales, Fuerzas y Cuerpos de Seguridad del Estado, Secretaria de Estado de Telecomunicaciones, Agencia Española de Protección de Datos, Red.es, Instituto Nacional de Tecnologías de la Comunicación, etc.) las recomendaciones que se proponen por los expertos a las autoridades se catalogan desde el:

  - *Punto de vista normativo:* a) instauración de una legislación que regule las transacciones comerciales y los flujos monetarios en la Red, exigiendo un sistema de autenticación fuerte (token de seguridad, DNI electrónico); b) completar la norma LSSI-CE respecto a la obligación de conservar los datos por parte de los operadores, c) la normalización de la protección del software, d) la armonización legislativa a nivel europeo en la tipificación de delitos y procedimientos jurídicos.

  - *Punto de vista ejecutivo y administrativo*: a) definición de un "superente" dentro de la Administración que aglutine funciones de asesoramiento al gobierno en materia legislativa, gestión de dominios, centro de alertas y respuesta a incidentes, con capacidad para proponer normativa, facultades de arbitraje y capacidad para establecer medidas cautelares y de persecución internacional; b). coordinación y participación activa de la Administración con el resto de agentes intervinientes en el proceso, etc.

- *Punto de vista formativo y divulgativo*: a) realización de un diagnóstico y seguimiento sobre el fraude online, b) impulsar medidas de prevención destinadas a fomentar la concienciación de los usuarios en el buen uso de Internet a través de una formación e información, c) impulsar la formación continua del usuario en temas relacionados con la seguridad en Internet (utilización de software legal, antivirus, actualización de las medidas de seguridad), d) foro de encuentro y debate para todos los agentes.

- **Dirigidas a los usuarios y asociaciones de consumidores y usuarios**: las recomendaciones generales que los expertos dirigen a este grupo de agentes tienen el objeto de evitar los ataques en sus dos principales lugares de origen: a) en relación con la ingeniería social las propuestas de actuación van enfocadas a promover la utilización de la cautela y el sentido común por parte del usuario, b) por lo que se refiere a las vulnerabilidades del sistema, los expertos insisten en mejorar la protección de nuestros sistemas así como mejorar los hábitos de seguridad de los usuarios.

Por lo que se refiere a las recomendaciones avanzadas cabe señalar el DNI electrónico como medida más valorada por los expertos; también se mencionan las tarjetas virtuales y de coordenadas, los token, el filtrado de correo, etc.

1 INTRODUCCIÓN, OBJETIVOS Y METODOLOGÍA

1.1 Presentación

1.1.1 El Instituto Nacional de Tecnologías de la Comunicación

El Instituto Nacional de Tecnologías de la Comunicación (INTECO), sociedad estatal promovida por el Ministerio de Industria, Turismo y Comercio, es una plataforma para el desarrollo de la Sociedad del Conocimiento a través de proyectos del ámbito de la innovación y la tecnología.

Su objetivo es doble: por una parte, contribuir a la convergencia de España con Europa en la Sociedad de la Información y, de otra parte, promover el desarrollo regional, enraizando en León un proyecto con vocación global.

La misión de INTECO es impulsar y desarrollar proyectos de innovación relacionados con el sector de las Tecnologías de la Información y la Comunicación (TIC) y en general, en el ámbito de la Sociedad de la Información, que mejoren la posición de España y aporten competitividad, extendiendo sus capacidades tanto al entorno europeo como al latinoamericano. Así, el Instituto tiene la vocación de ser un centro de desarrollo de carácter innovador y de interés público a nivel nacional que constituirá una iniciativa enriquecedora y difusora de las nuevas tecnologías en España en clara sintonía con Europa.

El objeto social de INTECO es la gestión, asesoramiento, promoción y difusión de proyectos tecnológicos en el marco de la Sociedad de la Información. Para ello, INTECO desarrollará actuaciones, al menos, en líneas estratégicas de Seguridad Tecnológica, Accesibilidad, Innovación en soluciones TIC para la Pyme, e-Salud, e-Democracia.

1.1.2 El Observatorio de la Seguridad de la Información

El Observatorio de la Seguridad de la Información se inserta dentro de la línea estratégica de actuación de INTECO en materia de Seguridad Tecnológica. El Observatorio nace con el objetivo de describir de manera detallada y sistemática el nivel de seguridad y confianza en la Sociedad de la Información y de generar conocimiento especializado en la materia. De este modo, se encuentra al servicio de los ciudadanos, las empresas y las administraciones públicas españolas para describir, analizar, asesorar y difundir la cultura de la Seguridad de la Información y la e-Confianza.

El Observatorio ha diseñado un Plan de Actividades y Estudios con el objeto de generar conocimiento especializado y útil en materia de seguridad por parte de INTECO, así como de elaborar recomendaciones y propuestas que definan tendencias válidas para la toma de decisiones futuras por parte de los poderes públicos.

Dentro de este plan de acción se realizarán labores de investigación, análisis, estudio, asesoramiento y divulgación que atenderán, entre otras, a las siguientes estrategias:

- Elaboración de estudios e informes propios en materia de seguridad de las Tecnologías de la Información y la Comunicación, con especial énfasis en la Seguridad en Internet.

- Seguimiento de los principales indicadores y políticas públicas relacionadas con la seguridad de la información y la confianza en el ámbito nacional e internacional.

- Generación de una base de datos que permita el análisis y evaluación de la seguridad y la confianza con una perspectiva temporal.

- Impulso de proyectos de investigación en materia de seguridad TIC.

- Difusión de estudios e informes publicados por otras entidades y organismos nacionales e internacionales, así como de información sobre la actualidad nacional y europea en materia de la seguridad y confianza en la Sociedad de la Información.

- Asesoramiento a las Administraciones Públicas en materia de seguridad de la información y confianza, así como el apoyo a la elaboración, seguimiento y evaluación de políticas públicas en este ámbito.

1.2 Objetivos del Estudio

La e-confianza de los ciudadanos respecto a Internet – y por tanto, no solo la incorporación sino la consolidación de los usuarios respecto los servicios de la Sociedad de la Información – está amenazada por una práctica delictiva denominada *phishing*.

Los ataques de *phishing* usan la ingeniería social para adquirir fraudulentamente de los usuarios información personal (principalmente de acceso a servicios financieros). Para alcanzar al mayor número posible de víctimas e incrementar así sus posibilidades de éxito, utilizan el correo basura (*spam*) para difundirse. Una vez que llega el correo al destinatario, intentan engañar a los usuarios para que faciliten datos de carácter personal, normalmente conduciéndolos a lugares de Internet falsificados, páginas web, aparentemente oficiales, de bancos y empresas de tarjeta de crédito que terminan de convencer al usuario a que introduzca datos personales de su cuenta bancaria, como su número de cuenta, contraseña, número de seguridad social, etc.

En este contexto, el Instituto Nacional de Tecnologías de la Comunicación (INTECO), se planteó la necesidad de realizar una investigación que permitiera:

- Conocer el punto de vista que tienen los usuarios y profesionales de las entidades afectadas por este fenómeno.

- Servir de base para orientar futuras iniciativas públicas y privadas en esta materia.

En este sentido, el estudio tiene unos objetivos amplios que se concretan en unos objetivos generales y unos objetivos operativos que se detallan a continuación:

Objetivos generales

1. Identificar las percepciones del *phishing* desde una perspectiva tecnológica, legislativa y social, no "contaminada" por la perspectiva de "vender soluciones", sino por la de definir demandas de actuación de los diversos colectivos afectados.

2. Definir tanto la problemática como las diversas soluciones que plantean los consultados respecto al *phishing*.

3. Orientar, con las conclusiones obtenidas de la investigación, iniciativas de carácter público y privado.

Objetivos operativos

1. Situación actual del fenómeno del *phishing* y las nuevas tendencias del fraude electrónico:

    a. Origen del fraude.

    b. Importancia cualitativa y cuantitativa del *phishing* y de otros fraudes en la Red.

    c. Objetivos de los delitos informáticos (robo de información sensible, robo de identidad, fraude económico).

    d. Formas de ataque (correo electrónico, código malicioso, sms o móvil, fax, otros).

    e. Impacto en los medios de comunicación.

2. Marco legal e implicaciones jurídicas.

3. Impacto económico y social del *phishing*.

4. Impacto en los agentes implicados en el proceso.

5. Conclusiones y recomendaciones de actuación.

1.3 Diseño metodológico

A continuación, se describe el proceso metodológico empleado en la elaboración del Estudio.

Fase de investigación.

La metodología empleada en esta fase consta de 3 etapas:

i) **Búsqueda y análisis documental** donde se han considerado numerosos estudios y artículos del ámbito nacional e internacional.

ii) Realización de **40 entrevistas en profundidad con expertos de los distintos sectores de actividad** relacionados con la seguridad y el intercambio de información a través de la Red, como principales sujetos afectados por el fenómeno del *phishing*, con el fin de establecer las perspectivas y el marco de análisis. Estas entrevistas han sido distribuidas entre los siguientes perfiles:

- Administración Pública
- Fuerzas y Cuerpos de Seguridad del Estado
- Abogados, juristas y expertos en derecho
- Entidades Financieras
- Proveedores de Servicios
- Asociaciones de Usuarios
- Medios de Pago
- Proveedores de Seguridad
- Operadores de Telefonía, DSL, y Voz IP

iii) Realización y análisis de resultados de **3.076 encuestas a usuarios** pertenecientes a hogares conectados a Internet sobre el fenómeno del fraude online[6]. Las características del trabajo de campo de dicha encuesta se describen seguidamente:

- Universo: Usuarios españoles de Internet, con acceso frecuente a Internet desde el hogar, mayores de 15 años. Para delimitar con mayor precisión el

[6] Los datos de los resultados cuantitativos obtenidos de la muestra, tienen su base en opiniones y percepciones de los usuarios encuestados.

concepto de usuario, se exige una conexión a Internet desde el hogar de al menos una vez al mes.

- Tamaño y distribución muestral: Se ha extraído una muestra representativa de 3.076 usuarios de Internet, mediante afijación muestral según un modelo polietápico:

- Estratificación por Comunidades Autónomas para garantizar un mínimo de sujetos en cada una de estas entidades.

- Muestreo por cuotas de tamaño del hogar, edad, sexo, actividad laboral y tamaño del hábitat[7].

Tabla 1: Distribución muestral por CCAA (%)

CCAA	Muestra Obtenida	Muestra Teórica
Andalucía	14,4	16,3
Aragón	3,4	2,9
Asturias	4,0	3,0
Baleares	2,4	2,5
Canarias	3,6	4,8
Cantabria	1,4	1,5
Castilla-La Mancha	2,8	3,9
Castilla y León	6,2	5,6
Cataluña	17,3	16,8
País Vasco	4,5	5,6
Extremadura	1,1	1,7
Galicia	5,2	5,8
Madrid	19,1	15,7
Murcia	2,3	3,0
Navarra	1,2	1,4
La Rioja	0,7	0,7
Comunidad Valenciana	10,4	8,8

Fuente: INTECO

Aunque las desviaciones entre la muestra obtenida y la teórica han sido pequeñas, la Muestra se ha equilibrado al universo en base a los datos poblacionales por CCAA, para el universo descrito anteriormente, y a las variables de cuota, para alcanzar un ajuste más perfecto.

[7] Estas cuotas se han obtenido de datos representativos a nivel nacional de internautas mayores de 15 años que se conectan más de una vez al mes desde el hogar facilitados por Red.es, entidad pública empresarial del Ministerio de Industria, Comercio y Turismo. ("Las TIC en los hogares españoles: 11ª Oleada-Octubre 2006")

Tabla 2: Distribución muestral por categorías sociodemográficas (%)

Concepto	Muestra Obtenida	Muestra Teórica
Actividad		
Ocupado	69,2	63,2
Parado	5,0	6,2
Estudio	19,0	22,8
Jubilado	2,2	2,8
Otros Inactivos	4,6	5,0
Tamaño hogar		
1	7,6	4,9
2	25,7	15,2
3	27,4	26,6
4 y más		
Sexo		
Hombre	47,3	52,2
Mujer	52,7	47,8
Hábitat		
Hasta 20.000	23,1	29,5
De 20.001 a 100.000	22,8	24,5
Más de 100.000 y capitales	54,1	46,0
Edad		
Hasta 24	25,4	25,5
De 25-35	40,0	29,5
De 35-49	27,2	30,6
De 50 y mas	7,3	14,4

Base muestra Enero= 3.035 Base muestra Abril=3.076 *Fuente: INTECO*

- Captura de información: Entrevistas online a partir de un panel de usuarios de Internet con un total 3.076 encuestados

- Trabajo de campo: Realizado en Abril de 2007.

- Error muestral: De acuerdo con los criterios del muestreo aleatorio simple para variables dicotómicas en las que p=q=0,5 y para un nivel de confianza del 95,5%, se establece el siguiente cálculo del error muestral:

  Muestra total n= 3.076, error muestral ±1,80%

Fase de análisis y debate de las conclusiones.

Conjugando los resultados y los datos obtenidos en la fase previa se elaboró a modo de resumen un **Informe Previo de Conclusiones,** cuyos resultados fueron **debatidos en dos grupos representativos de los agentes y perfiles entrevistados**. Estas entrevistas han sido distribuidas entre los siguientes perfiles: (entidades financieras, empresas

prestadoras de servicios a través de Internet, medios de pago, fabricantes y proveedores de soluciones de seguridad, Administración Públicas, Fuerzas y Cuerpos de Seguridad del Estado, abogados, juristas y expertos en Derecho, y asociaciones de consumidores y usuarios). Sus conclusiones retroalimentaron aquellos resultados, dando origen al Informe de Conclusiones definitivas.

Fase de recomendaciones de actuación.

Sobre la base de este último informe, se han identificado las recomendaciones y orientaciones de actuación expuestas por los propios afectados con el objeto de, en primer lugar, mejorar el protocolo de actuación en el caso de ser afectados (ciudadanos, empresas o administraciones) por esta práctica fraudulenta; y, en segundo lugar, poder ser empleadas como medidas preventivas ante la proliferación de otras amenazas informáticas de similar naturaleza.

1.3.1 Estructura de contenidos

El Estudio se estructura en la siguiente forma:

- En primer lugar, el estudio expone el **origen, definición, tipología y evolución** de la práctica fraudulenta conocida como *phishing* dentro de la panorámica global del fraude a través de la Red, incluyéndose su **impacto económico y social** (Capítulo 2 del Estudio).

- En segundo lugar, se presentan los resultados de la fase cuantitativa de la investigación, aportándose **datos estadísticos sobre la percepción del fraude online** recogidos a través de más de 3.000 encuestas realizadas a usuarios habituales de Internet de toda España (Capítulo 3).

- A continuación se aborda el **posicionamiento y papel de los agentes afectados** por el fenómeno del phishing, tanto entidades públicas como privadas, contemplando cuál es su **situación actual y qué medidas de actuación** concretas están llevando a cabo (Capítulo 4).

- En un cuarto bloque del estudio incluye el análisis de los resultados de la **fase cualitativa** del Estudio: las entrevistas y dinámicas de grupo realizadas durante la investigación a los expertos de todos los sectores de actividad afectados, identificando las principales **propuestas y recomendaciones** para afrontar esta práctica fraudulenta por cada uno de los agentes implicados. En concreto, este epígrafe (Capítulo 5) recoge la visión prospectiva y tendencias dadas por los propios agentes, así como las líneas de actuación genéricas y avanzadas identificadas para todos ellos.

- Finalmente, el documento recopila las **conclusiones** del Estudio (Capítulo 6) y numerosas **referencias bibliográficas** (Capítulo 7).

2 LA UTILIZACIÓN ILÍCITA DE INTERNET

La informática y las comunicaciones, muy especialmente con la popularización de Internet, han cambiado, en muchos casos radicalmente, la forma de trabajar y de disfrutar del tiempo libre. A principios de los años 80, incluso en los países más desarrollados, habría sido muy difícil imaginar muchas de las acciones cuya realización a través de la Red hoy resultan cotidianas.

Estos indudables avances también han traído consigo consecuencias no deseadas; en este caso, la proliferación de agentes que aprovechan los recursos del sistema y la buena intención del resto de actores para buscar ilícitamente el beneficio propio o del daño a terceros. De esta forma nacen los delitos informáticos, delitos electrónicos, delitos telemáticos o ciberdelitos.[8]

2.1 El delito informático

2.1.1 Definición del delito informático

Se puede considerar que delito informático es cualquier tipo de conducta tipificada como delictiva para cuya comisión se utilicen tecnologías de información y/o comunicaciones[9].

A partir de las diferentes fuentes jurídicas pueden identificarse determinadas características de los delitos informáticos:

- **Transnacionalidad**. Los delitos informáticos trascienden las fronteras de los estados, lo que hace recomendable regulaciones también transnacionales de este tipo de actividades criminales.

- **Distancia física**. Los delincuentes nunca están en el "lugar del crimen" físicamente, por lo que su localización es más compleja y el riesgo que asumen es menor.

- **Ubicuidad**. Es posible cometer delitos de forma simultánea en lugares muy distantes.

- **Complejidad derivada de la profesionalización y redes organizadas de ciberdelincuentes:** En numerosos casos las actividades fraudulentas son llevadas a cabo por mafias y redes de delincuentes organizadas y especializadas,

[8] Aunque pueden existir diferencias de matiz entre algunas de estas denominaciones, como podría ser la utilización o no de conexiones a Internet, en la actualidad el número e impacto de los delitos informáticos que no utilicen este tipo de conexiones, aunque posible, es prácticamente nulo.

[9] Esta definición trata de resumir las muchas existentes. Una discusión más detenida del término "ciberdelito" o delito electrónico puede encontrarse en Sánchez Magro, A. (2005).

frecuentemente ubicadas muy lejos de nuestras fronteras y con un entramado desatomizado, complejo y opaco.

De todas estas cuestiones, posiblemente la transnacionalidad es la más preocupante: un delincuente chino puede cometer una estafa en Estados Unidos estando físicamente en Italia a través de una red de ordenadores zombis (controlados remotamente) localizados en Rusia. Así pues, la complejidad procesal resultante de la coexistencia de diferentes tipos delictivos y la aplicabilidad de diversas legislaciones puede dificultar la persecución del delito.

En base a las soluciones tradicionales, se suele abogar por la **persecución del delito** por parte de las **autoridades del país en el que la víctima sufre sus consecuencias**. Esta situación tiene una cierta utilidad práctica, que ha conducido a un relativo consenso en torno a su adopción.

2.1.2 Tipos de delitos informáticos

Dado lo novedoso y la constante evolución de las formas delictivas a través de redes de comunicaciones, no existe una tipología universal de los delitos informáticos. Así, se plantean diferentes clasificaciones, según diversos criterios.

Una primera clasificación distinguiría entre los **delitos que tienen su origen en técnicas de ingeniería social y los que tratan de aprovecharse de vulnerabilidades de los sistemas**. No obstante, en algunos ciberdelitos se combinan ambos orígenes.

- Los delitos basados en técnicas de ingeniería social son relativamente similares a los tradicionales “timos”, en los que se engaña a la víctima para que haga algo (revelar información sensible de carácter personal e incluso cometer él mismo- de manera inconsciente- la actividad delictiva) que normalmente no haría y que va a ocasionar un perjuicio económico, ya sea a él o a terceros. Entre ellos destaca cuantitativamente el fraude denominado *phishing*, junto a otros como las llamadas “cartas nigerianas”, el *scam* y otras modalidades.

- Los delitos que se aprovechan de vulnerabilidades en el sistema requieren normalmente una habilidad mayor por parte del delincuente, ya que parten de la utilización (y en ocasiones creación) de programas que aprovechen los fallos de sistema de información para causar daños. Además, no requieren de la “colaboración” de la víctima, ya que ésta, sin haber omitido ninguna norma de seguridad, puede verse perjudicada a través de un tercero. En este grupo podríamos situar al *pharming* y al más tradicional *hacking*.

Otra clasificación interesante puede basarse en el **objeto de los delitos informáticos**. En este sentido, se pueden distinguir los delitos sobre las personas, los delitos sobre la propiedad privada y los delitos sobre las autoridades.

- Respecto a los delitos informáticos ejercidos sobre personas, en su mayoría son las versiones cibernéticas de algunas conductas tradicionalmente tipificadas como delictivas. Se pueden situar dentro de este grupo el acoso de cualquier tipo, las amenazas, las injurias o la pederastia.

- Los delitos informáticos sobre la propiedad se equiparan prácticamente a la mayor parte de formas de fraude tradicionales, aunque en algún caso las nuevas herramientas tecnológicas han permitido crear algunos nuevos tipos. Se incluyen dentro de este grupo todo tipo de violaciones de la propiedad, no sólo referidas al dinero (*phishing*, *scam*, "cartas nigerianas", *pharming*, etc.), sino a la propiedad intelectual ("crackeo" o creación de software destinado a facilitar la supresión no autorizada o la neutralización de cualquier dispositivo técnico que se haya utilizado para proteger programas de ordenador).

- Finalmente, un tercer grupo de delitos informáticos puede tener como objetivo atacar a las autoridades de un país y, en definitiva, al sistema socio-económico de éste. Es el conocido como ciberterrorismo[10], afortunadamente muy poco frecuente.

2.1.3 El delito informático en el ordenamiento jurídico español

A la hora de valorar el tratamiento jurídico de los delitos informáticos conviene anticipar dos premisas:

a) Existe entre los juristas un cierto debate acerca de la propia existencia jurídica de los delitos informáticos. Algunas posiciones sostienen, de manera clara, que el ciberdelito no existe, dado que se reduce al mero hecho de ser cometido sobre o mediante el ordenador. En este sentido, no sería necesario un tratamiento específico por parte de los ordenamientos jurídicos.

   Sin embargo, quizás por puro pragmatismo, la mayor parte de los juristas consideran necesaria una tipificación específica de estos delitos, debido a la existencia de una nueva realidad como son las autopistas de la información. Este último parece ser el camino seguido no sólo por el ordenamiento penal español, sino por la mayoría de los correspondientes a países de nuestro entorno.

b) Una segunda decisión consiste bien en separar los delitos informáticos de los delitos tradicionales a través de un tratamiento diferenciado, o bien la decisión de una regulación conjunta.

[10] Ejemplo de este grupo de delitos informáticos es el caso acontecido a mediados de mayo de 2007 en el cual el Ministro de Defensa estonio, Jaak Aaviksoo, comparaba con una acción terrorista los últimos ataques contra la embajada estonia en Moscú y varios asaltos informáticos contra empresas e instituciones que llevaron al Gobierno de Tallin a solicitar ayuda a la OTAN.

El legislador español se ha decantado por una regulación no autónoma, de modo que no existe en el Código Penal de 1995 un título propio relativo a los delitos informáticos insertándose su tipificación en los correspondientes a los delitos tradicionales.

A continuación se recoge un análisis de los delitos informáticos contemplados en el Código Penal español, donde se pueden encontrar los siguientes tipos:

Delitos de naturaleza económica

Se puede considerar dentro de este grupo los que afectan patrimonialmente a otras personas, o aquellos que generan perjuicios al funcionamiento del orden económico en general.

Dentro de este grupo, el delito más habitual -por cuanto engloba una amplia variedad de conductas delictivas- es la estafa informática. Regulada en el artículo 248 del Código Penal, en su apartado 1 se distingue entre los supuestos de estafa basados en técnicas de ingeniería social pura (donde se sitúa el *phishing*): "*Cometen estafa los que, con ánimo de lucro, utilizaren engaño bastante para producir error en otro, induciéndolo a realizar un acto de disposición en perjuicio propio o ajeno*"; y los supuestos de utilización de código malicioso (*malware*) o de intrusión en sistemas de información recogidos en el artículo 248.2 del CP: "*También se consideran reos de estafa los que, con ánimo de lucro, y valiéndose de alguna manipulación informática o artificio semejante consigan la transferencia no consentida de cualquier activo patrimonial en perjuicio de tercero*".

El legislador contempla también la posibilidad de delito en grado de tentativa en un tercer apartado del artículo, por lo que la posesión o distribución de programas maliciosos (*malware*) en sí misma podría ser constitutiva de delito.

No obstante, hay que recordar que algunas de las aplicaciones cuya finalidad más habitual es delictiva admiten utilizaciones legales, por lo que su persecución podría ser más difícil porque el precepto legal habla de aplicaciones destinadas específicamente a los fines ilícitos.

Las penas establecidas por el artículo 249 y los agravantes recogidos en el artículo 250 reflejan la realidad de un delito contra el patrimonio.

El artículo 264 establece como delito los daños a la propiedad en general, y los daños informáticos en particular en su apartado 2.

Uno de los delitos informáticos de más actualidad, de contenido económico, son los daños a la propiedad intelectual. El artículo 270 del Código Penal realiza un amplio recorrido por las conductas punibles, aunque siempre deja abierta la puerta a la determinación de éstas, dado que es imposible fijar todos los contenidos a priori.

Finalmente, dentro de los delitos con contenido patrimonial hay que situar la regulación de los secretos de empresa, recogida en el artículo 278.1 del Código Penal. Este delito es agravado por la difusión (artículo 278.2).

Asimismo, incurre en este tipo de delito el que difunde la información – estando obligado a guardarla (artículo 279) – y el que la utiliza en provecho propio – sabiendo de su procedencia ilegal (artículo 280) – para tratar de evitar que alguien que puede encargar a un tercero la comisión de este tipo de delito, saque provecho de ello y quede finalmente impune.

Delitos de falsedad documental

Se puede considerar que la falsificación de soportes informáticos que presten el apoyo documental a diferentes tipos de transacciones cae dentro de los supuestos del delito de falsedad documental, regulado en todas sus versiones en los artículos 390 a 399 del Código Penal. De hecho, los soportes informáticos se ajustan perfectamente a la definición de documento que proporciona el propio Código Penal.

Otras infracciones reguladas por la legislación española

Actualmente el *spam* está prohibido por el artículo 21.1 de la Ley de Servicios de la Sociedad de la Información y de Comercio Electrónico (LSSI-CE). El enunciado específico de este artículo afirma que "queda prohibido el envío de comunicaciones publicitarias o promocionales por correo electrónico u otro medio de comunicación electrónica equivalente que previamente no hubieran sido solicitadas o expresamente autorizadas por los destinatarios de las mismas", exponiendo en el punto 2 de este artículo que sí se admite este tipo de envíos, siempre y cuando hubiera una relación contractual previa.

Posteriormente, el artículo 38.3 de esta misma ley cataloga el *spam* como infracción grave, siempre que el autor contacte con más de tres destinatarios. Una infracción grave lleva aparejada una multa entre los 30.001€ y los 150.000€[11]. De este modo, el *spam* no es considerado un delito, esto es, no es objeto de regulación penal, sino motivo de una sanción. La **Agencia Española de Protección de Datos** (www.agpd.es) es, en virtud de la Ley General de Telecomunicaciones (LGT), el órgano garante del cumplimiento de la LSSI-CE y, por tanto, la encargada de imponer multas derivadas de las infracciones (art. 43.1 de LSSI-CE).

Es especialmente interesante la llamada acción de cesación, consistente en instar al causante a interrumpir su actividad. Además, la Ley plantea mecanismos ágiles para la

[11] Si se envían menos de tres mensajes, se incurre en una infracción leve, con multas de hasta 30.000€.

resolución extrajudicial de conflictos, acordes con la realidad de la Sociedad de la Información.

La Agencia Española de Protección de Datos señala que el *spam* podría ser considerado también un incumplimiento de la legislación sobre protección de datos, ya que requiere el acceso a la dirección de correo electrónico, que podría ser considerada un dato de carácter personal[12]. En este sentido, la obtención de datos de carácter personal sin, consentimiento o su utilización para fines no autorizados, se considera infracción grave en la mayor parte de los casos, con multas entre los 60.000€ y los 300.000€. Nuevamente, se trata de una infracción sancionada por un órgano administrativo, y no de un delito.

La Agencia de Protección de Datos es quizás la pieza fundamental de esta norma, con amplias funciones de carácter registrador, legislativo, inspector, sancionador y representativo. No obstante, como se ha indicado, no tiene potestad para imponer sanciones de orden penal.

Por otro lado, la Directiva sobre Privacidad de las Telecomunicaciones de la Unión Europea (Directiva 58/2002/CE), transpuesta al derecho español por la Ley General de Telecomunicaciones (Ley 32/2003) establece, de forma similar a la LSSI-CE, el principio de consentimiento previo, que requiere éste para el envío de correo electrónico con fines comerciales, nuevamente salvo que existiese una relación previa. Las legislaciones de la mayor parte de países pertenecientes a la OCDE tienen normas que prohíben el *spam*.

2.1.4 La relación entre el correo electrónico no deseado (*spam*) y las prácticas delictivas a través de Internet.

Caracterización del correo no deseado (*spam*)

Hoy día resulta habitual que los usuarios de correo electrónico reciban una importante cantidad de mensajes no solicitados y, en muchos casos, inútiles o incluso perjudiciales que tratan de persuadirles de la necesidad de llevar a cabo una determinada acción, les cuentan alguna historia más o menos verosímil, publicitan un producto específico o comunican un hecho.

La Agencia Española de Protección de Datos denomina *spam* a “cualquier mensaje no solicitado y que normalmente tiene el fin de ofertar, comercializar o tratar de despertar el interés respecto de un producto, servicio o empresa”. Se afirma, además, que la vía más común para este tipo de práctica es el correo electrónico.

[12] Si bien en muchas ocasiones las direcciones de correo electrónico de los empleados son públicamente disponibles a través de las páginas web corporativas.

Se puede decir que esta definición carece de uno de los componentes que suele considerarse más habitual en el *spam*, como es su carácter masivo, esto es, su envío a múltiples destinatarios. De esta forma, se puede considerar *spam* a los mensajes no solicitados enviados en cantidades masivas a un número muy amplio de usuarios.

En relación con los tipos de *spam*, partiendo de diferentes clasificaciones, como la utilizada por la propia Agencia Española de Protección de Datos, se puede distinguir diferentes modalidades en función de su contenido:

- El *spam* con fines comerciales. Se trata del pionero, y tiene como objetivo difundir la utilidad de un producto o la posibilidad de adquirirlo a un precio inferior al de mercado. En algunos casos, tiene relación con algunos tipos delictivos, ya que en la actualidad se están ofertando por este método productos que infringen las leyes de propiedad intelectual, de patentes o normativas sanitarias (se ofrecen medicamentos, relojes y joyas, música…).

- El bulo (en inglés *hoax*). Mensaje de correo electrónico con contenido falso o engañoso, generalmente enviados encadenadamente y que solicita al receptor reenvíos posteriores continuando dicha cadena. En ellos se cuenta una historia más o menos verosímil relativa a injusticias, abusos, problemas sociales o fórmulas para alcanzar determinado bienestar. El bulo persigue captar direcciones de correo electrónico (que se van acumulando en el proceso de reenvío) para ser utilizadas posteriormente como objeto del *spam*. También se suele afirmar que el objetivo de este tipo de mensajes es motivar el gasto de recursos de los sistemas de información y comunicaciones. Existe un problema con su regulación legal, ya que no constituye en sí mismo una infracción de la ley, al no tratarse de comunicaciones comerciales.

- El *spam* con fines fraudulentos. El *spam* puede ser, en muchos casos, la cabeza de puente para la comisión de un fraude. De esta forma, la mayor parte de los intentos de *phishing*, "cartas nigerianas"[13], *scam* y otras modalidades fraudulentas llegan a sus destinatarios a través de su correo electrónico, a la vez que han sido enviados masivamente a otros destinatarios.

- El *spam* con otros fines delictivos. A medio camino entre el *hoax* y el fraude, a través de un ataque de *spamming* se puede tratar de dañar la reputación de una persona física o jurídica, muy especialmente si los destinatarios de este tipo de mensaje son sensibles a su contenido. De este modo, estos mensajes masivos suelen ser un medio utilizado para propagar rumores con muy escasa verosimilitud,

[13] Se ofrece un negocio fácil y con suculentos beneficios y se solicita a la victima un anticipo económico para afrontar los gastos iniciales.

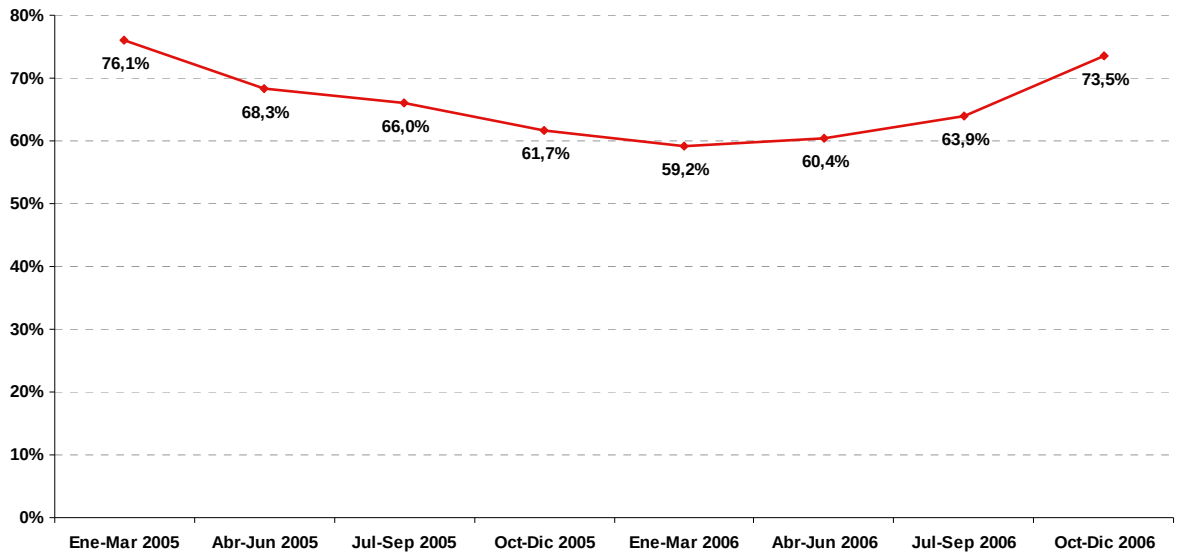
de los que se desconoce el verdadero origen, a pesar de ser recibidos por parte de algún conocido.

La magnitud del correo no deseado (*spam*) en la actualidad

El volumen actual de correo no deseado es difícil de comprender para cualquier usuario no habitual. Según datos recientes (

Gráfico 1), en la actualidad, casi tres de cada cuatro mensajes (73,5%) de correo electrónico son *spam*. A pesar de no suponer una gran ocupación del ancho de banda, resulta una molestia y una pérdida de tiempo para las empresas.

Gráfico 1: Magnitud a nivel mundial del *spam* durante 2005 y 2006 (%)



Fuente: MessageLabs (2007)

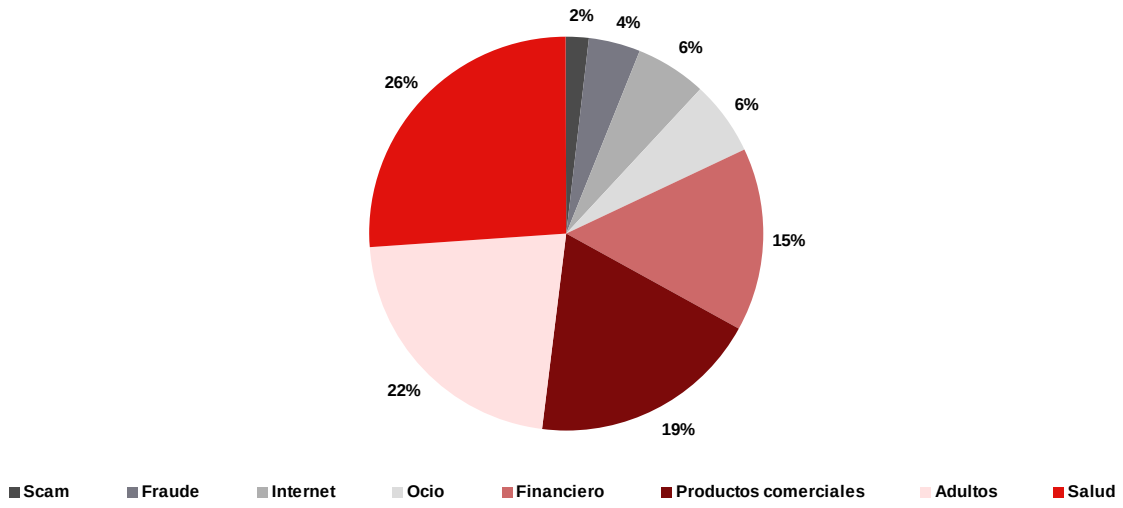
El espectacular crecimiento de este fenómeno tiene varios orígenes. Por una parte, la disponibilidad más amplia de mejores redes de comunicaciones y un creciente e importante número de conexiones a Internet en la práctica totalidad de los países miembros de la **Organización para la Cooperación y Desarrollo Económico –OCDE-** (www.oecd.ord) hace que este tipo de práctica tenga un elevado número de objetivos potenciales.

Las redes de ordenadores zombis o *botnets*[14] también han contribuido al crecimiento exponencial del *spam*; gran parte del *spam* actual es enviado por estas redes.

[14] Las botnets o redes de ordenadores zombis se basan en el empleo de un programa de código malicioso que se instala sin permiso en el ordenador y por el cual este queda bajo el control (zombi) de un tercero para, por ejemplo, efectuar envíos

Más allá del volumen de *spam*, con la pérdida de recursos que puede suponer, hay que analizarlo como una potencial herramienta delictiva. Como muestra el Gráfico 2 aunque sólo un 4% de los mensajes *spam* aparece catalogado directamente como fraudulento, es preciso señalar que la apariencia financiera o comercial puede ser una simple máscara debajo de la cual se oculte una segunda fase de la estafa basada en la ingeniería social.

Gráfico 2: Tipología del contenido de los mensajes de *spam* a nivel mundial en 2006 (%).



Fuente: Symantec (2007)

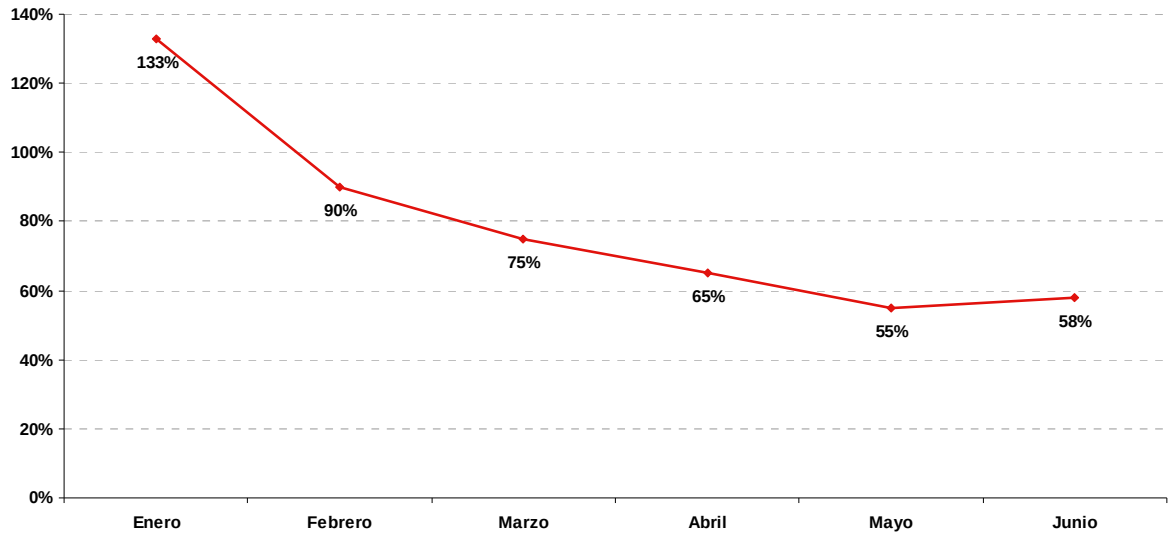
Relación entre el correo electrónico no deseado (*spam*) y el *phishing*

Respecto a la relación entre el *spam* y el *phishing*, parece claro que este tipo de mensajes de distribución masiva puede ser una eficiente forma de captación utilizada por los delincuentes. De hecho, como se verá más adelante, uno de los métodos más habituales de contacto para la comisión de delitos informáticos es el correo electrónico.

El porcentaje de mensajes de *spam* catalogados como *phishing* es bastante bajo, pero es preciso tener en cuenta que éstos sólo abarcan una tipología muy específica de fraude. Aun así, como se muestra a continuación en el Gráfico 3 existe una tendencia hacia la reducción del porcentaje de *phishing* localizado en correos electrónicos no solicitados.

masivos de correos electrónicos. Para más información, se recomienda la lectura del artículo "Amenazas silenciosas en la Red: *rootkit*s y *botnets*" elaborado por el Observatorio de la Seguridad de la Información de INTECO y disponible en www.inteco.es.

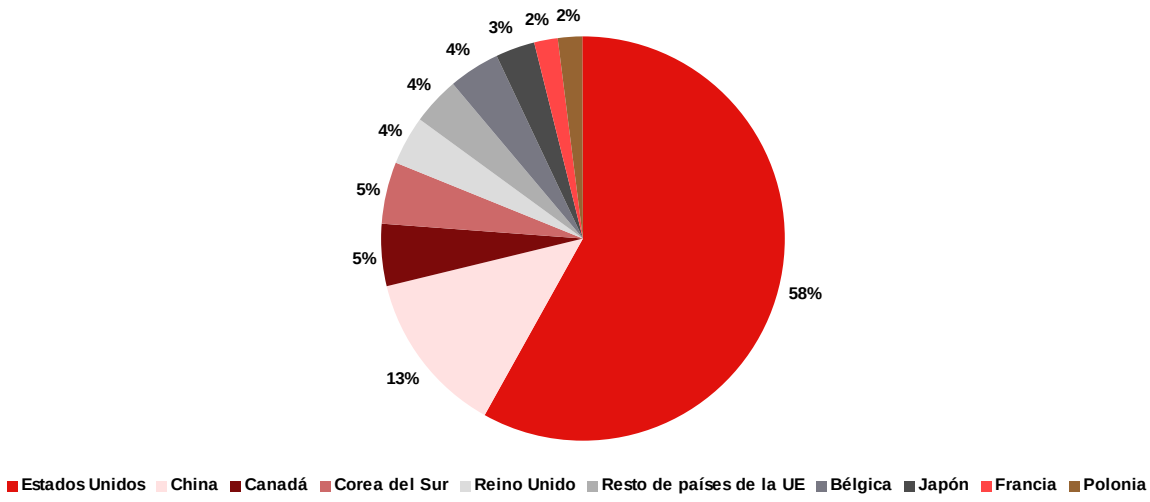
Gráfico 3: Evolución mundial del porcentaje de correo no deseado (*spam*) que incluye intentos de fraude online (*phishing*) - 1er semestre 2006



Fuente: Symantec (2007)

Otra información destacable que se recoge en el Gráfico 4 es la referida al origen de los mensajes de *spam*. Así, existe una alta correlación entre *spam* y *botnets* (*redes de ordenadores zombis*) capturadas, siendo habitualmente origen de este tipo de mensajes aquellos países con un mayor número de ordenadores controlados remotamente.

Gráfico 4: Distribución del *spam* considerado *phishing* según su origen geográfico (%).



Fuente: Symantec (2007)

Por otro lado, dado que el mensaje intenta atraer la confianza del receptor, se intenta en la mayoría de los casos su envío desde lugares que generen confianza. De este modo, en la lista de los "grandes remitentes" de *spam* cuyo objetivo es el *phishing* se encuentran, entre otros, Estados Unidos, Canadá, China y países de la UE.

2.2 El fraude informático.

2.2.1 Definición de fraude informático

El Convenio de Budapest del Consejo de Europa sobre Ciberdelincuencia recoge en su artículo 8 el fraude informático, considerando dentro del mismo "(…) los actos deliberados e ilegítimos que causen un perjuicio patrimonial mediante una amplia gama de procedimientos (…) con la intención fraudulenta o delictiva de obtener ilegítimamente un beneficio económico para uno mismo o para otra persona". Se puede considerar que esta sería, igualmente, la definición de estafa informática. [15]

Respecto a los tipos de fraudes a través de medios electrónicos, en la mayor parte de los casos, la legislación es poco explícita. Lo habitual es recoger tipos genéricos, en los que se puedan encajar los diferentes supuestos de estafa o fraude en Internet que puedan producirse.

Los elementos que concurren en el fraude a través de Internet son:

i) Voluntad.

ii) Carácter lucrativo.

iii) Perjuicio patrimonial del tercero.

iv) Utilización de medios electrónicos o informáticos para la comisión del delito.[16]

2.2.2 Clasificación del fraude informático

Es difícil realizar una clasificación sistemática del fraude electrónico. Una de las fuentes de datos más completa al respecto, es el **Internet Crime Complaint Center -IC3-** (www.ic3.gov). En ella se distinguen, a semejanza de nuestro código penal español, entre las estafas informáticas y las estafas tradicionales a través de medios informáticos.

[15] Profundizando en la terminología penal, existen algunas diferencias entre estafa y fraude. No obstante, a los efectos del estudio que nos ocupa, ambas coinciden en la voluntad dolosa de lucro a costa de otro mediante engaño.

[16] El Código Penal de 1995 hace una llamativa separación entre los supuestos de pura ingeniería social, que son tipificados en el mismo apartado que las estafas tradicionales, y los supuestos de utilización de código malicioso o de intrusión en sistemas de información. Aunque el legislador no pretende hacer una distinción técnica, de hecho la está haciendo.

Estafas tradicionales a través de medios electrónicos

Se trata de algunos de los fraudes y timos más tradicionales, "puestos al día" ante las amplias posibilidades de Internet. Su tratamiento penal se recoge en el artículo 248.1 del Código Penal, contemplándose como una estafa tradicional.

Junto al *phishing*, se encuentran dentro de esta categoría los siguientes ejemplos:

1.- El cheque de caja falso

Suele utilizarse cuando una persona vende un artículo en Internet. Un comprador, desde fuera del país donde se realiza la venta, se comunica con el vendedor para realizar la compra. Para pagar, se compromete a hacer llegar un cheque de caja por medio de alguien, generalmente un "socio", que le debe dinero. El importe del cheque suele ser muy superior al precio del artículo comprado. Al tratarse de un cheque de caja, el vendedor no suele tener problema para hacerlo efectivo en su sucursal.

El dinero sobrante debe ser utilizado para pagar los gastos de envío, y el remanente debe enviarse a través de transferencia bancaria o servicio de envío de dinero. Al cabo de unos días el banco descubre que el cheque era falso y, como consecuencia, la víctima tiene que pagar al banco el importe total del cheque.

2.- Las "cartas nigerianas"

Han recibido su nombre porque, en la mayor parte de los casos, afirman que proceden de África. Nuevamente, se trata de un fraude tradicional. El estafador se pone en contacto con la víctima, pidiendo ayuda para poder transferir fuera del país, por un determinado motivo, una cantidad de dinero o bienes valiosos. La víctima recibirá a cambio una comisión. Sólo tiene que abrir una cuenta en un banco extranjero y ayudar al estafador a "realizar los trámites"

El delincuente suele "cebar" a la víctima enviándole correos con documentos digitalizados que, teóricamente, son los resguardos de la operación. Pero algo interrumpe la transferencia: es necesario pagar una serie de gastos e impuestos, que el estafador afirma no poder pagar, y trata de convencer a la víctima de que envíe dinero con este cometido. La trama continúa hasta que la víctima deja de enviar fondos.

La estafa de la lotería

Mediante un correo electrónico se comunica a la víctima que ha sido agraciada con un premio de una lotería a la que no ha jugado. El premio le será transferido tras el envío de una serie de información (suficiente como para llegar a tomar el control de sus

cuentas financieras- encuadrándose dentro del *phishing*-) y de una cantidad de dinero para sufragar gastos.

La estafa de la hipoteca

Una entidad financiera, o broker financiero inexistente, se pone en contacto con la posible víctima, y le ofrece una hipoteca a un tipo de interés muy atractivo, sin importar su nivel de solvencia, y con muy escaso papeleo.

Para acceder a esta hipoteca se solicita a la víctima información, tanta como el estafador desee para futuros usos fraudulentos, y nuevamente dinero por adelantado, para pagar una serie de gastos.

Las pirámides de valor

Es un clásico entre las estafas que ha desembarcado en el mundo electrónico de la mano del *spam*. El estafador se pone en contacto con la víctima y le promete altos rendimientos para sus inversiones, para lo cual debe buscar nuevos inversores, y así sucesivamente, hasta que pueda cobrar su rentabilidad. El dinero siempre se obtiene de los nuevos entrantes. Al final, siempre ganan los mismos (los que originan la pirámide) y siempre pierden los mismos (los últimos que entran en ella).

Estafas esencialmente electrónicas

Requieren la utilización de medios informáticos o de comunicaciones para su comisión, esto es, las que serían perseguidas en virtud del artículo 248.2 del Código Penal. De este modo, forman parte de este grupo, todas las estafas que utilicen códigos maliciosos o métodos de intromisión ilegal en los sistemas de las empresas proveedoras de servicios a través de Internet, así como aquellas que requieran de medios electrónicos para su realización, es decir, que no tengan posibles versiones “pre-electrónicas”.

Se detallan a continuación algunos de los ejemplos más frecuentes:

1.- El fraude mediante subastas

Algunas páginas de Internet, como eBay (www.ebay.es), han contribuido a popularizar las subastas entre una buena cantidad de navegantes. No obstante, han sido también uno de los medios utilizados por los estafadores.

El fraude en las subastas es bastante sencillo. Se produce cuando una de las partes, generalmente el vendedor, no cumple con su compromiso, esto es, cobra pero no envía el bien. También es posible que sea el comprador el que trate de engañar, remitiendo a medios de pago que en la práctica no funcionan o no son suyos (tarjetas de crédito robadas). El problema de estos medios, a diferencia de las tarjetas de

crédito, es que una vez que la víctima ha caído en la trampa, no podrá recuperar su dinero.

En los últimos años, algunos de los servidores dedicados a subastas más populares en los Estados Unidos están siendo colapsados con ofertas de venta procedentes aparentemente de Estados Unidos, aunque luego requieren el pago a un familiar enfermo o a un socio de negocios residente en un país europeo, a través de los servicios de transferencia de dinero como MoneyGram o Western Union o, incluso mediante transferencia bancaria.

Quizás debido a su simplicidad el fraude en las subastas es considerado por algunos como "el rey" de los engaños en Internet, representando más de la mitad de los actos delictivos. Algunas recomendaciones del IC3 apuntan a desconfiar ante la falta de coincidencias en las direcciones postales, requerimientos de pago por medios diferentes a la tarjeta de crédito o solicitudes de envío a través de métodos poco habituales por parte del comprador.

El fraude de los medios de pago "*escrow*"

Ante la inseguridad de algunas compras realizadas a través de Internet, han nacido empresas consignatarias: el pago se realiza a estas empresas, y no se transfiere al vendedor hasta que el comprador ha obtenido el bien y muestra su conformidad.

Algunos estafadores han creado falsas empresas consignatarias. De este modo se consigue simultáneamente estafar al comprador (que pierde el dinero pagado) y desvelar algunos datos de información de personas que pueden ser relevantes en sucesivas estafas.

El fraude de los servicios de paquetería

Tras haber realizado una compra a través de Internet, especialmente a través de páginas de subastas, el estafador se pone en contacto con la víctima, haciéndose pasar por la empresa de mensajería que le va a llevar el producto. Con este fin, le pide una serie de datos. A partir de ahí, las variedades de esta estafa son muchas.

El fraude de la oferta de trabajo a distancia o *scam*

Se trata de una mezcla de *phishing* y pirámide de valor, realizada a través de medios electrónicos, generalmente partiendo de una oferta de teletrabajo.

La víctima accede a una oferta de trabajo, en la que se le promete un porcentaje de rentabilidad por poner objetos relativamente caros (TV de plasma, ordenadores potentes, etc.) a la venta en páginas de subastas o comerciales en Internet. La tarea del "primer estafado" es realizar estas ventas, y transferir el dinero, reteniendo en

ocasiones su porcentaje, a la teórica empresa para la que trabaja, que se encargará de enviar los bienes a los compradores.

En realidad, este intermediario está actuando de lo que se suele llamar "mula" o "mulero", transportando el dinero del segundo estafado al delincuente. Los bienes teóricamente vendidos nunca son entregados.

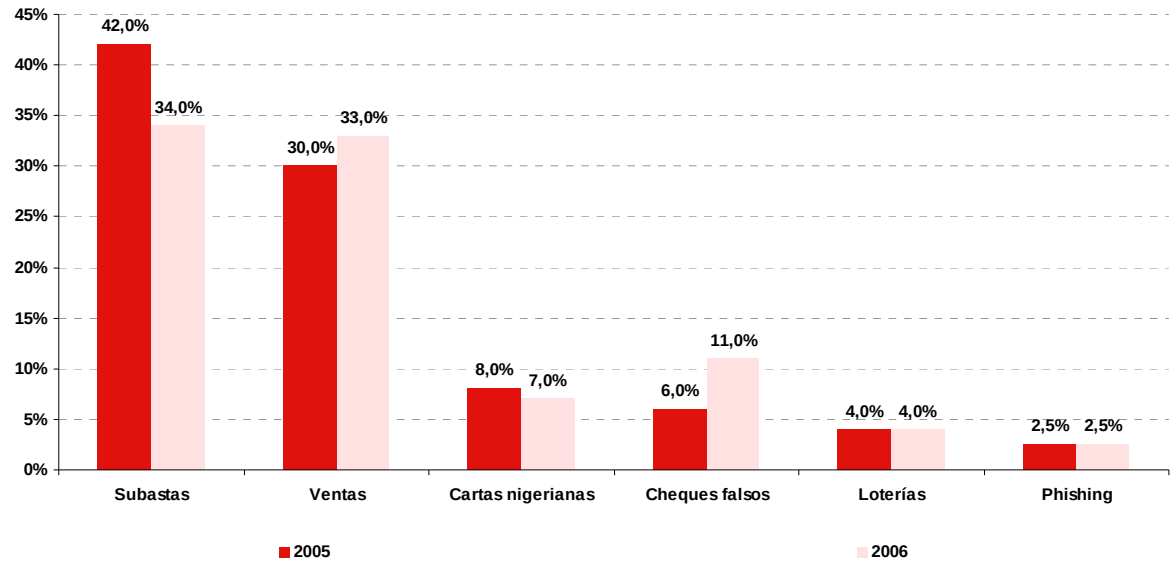
El fraude del reenvío

La víctima lee una oferta de empleo, a la que accede, proporcionando una gran cantidad de información personal.

La víctima empieza a recibir bienes, y se encarga de reenviarlos rápidamente al extranjero. Al poco tiempo, las autoridades comunican a la víctima que lo que realmente ha estado haciendo es contribuir al envío de mercancía comprada con tarjetas de crédito robadas mediante medios electrónicos.

En el Gráfico 5 se puede ver cómo las relacionadas con subastas y ventas a través de medios electrónicos son las estafas más habituales.

Gráfico 5: Principales tipos de estafas electrónicas en 2005 y 2006 en EEUU (%).

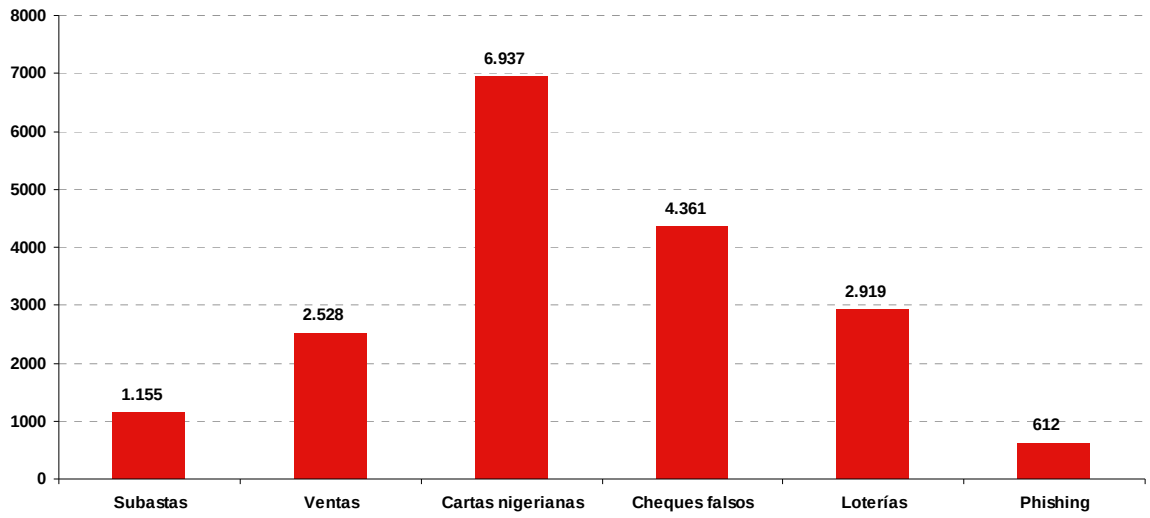


Fuente: Nacional Consumer League (2006)

La escasa relevancia del *phishing* en esta estadística se debe a que únicamente se considera éste en su sentido más estricto, separándose de otras prácticas bastante cercanas a la hora de realizar el análisis.

En el Gráfico 6 se observa que respecto a la pérdida media por estafa en EEUU en 2005, fueron las "cartas nigerianas" las que tuvieron un mayor importe acumulado. Hay que resaltar que los importes son, en todo caso, muy elevados, lo que da una prueba más de la importancia de la amenaza y de la necesidad de información de la opinión pública.

Gráfico 6: Pérdida media por estafa en función de su tipología (dólares)



Fuente: Nacional Consumer League (2006)

También es interesante analizar los medios de pago utilizados por los estafados durante los años 2005 y 2006. La nota común es que los estafados tratan de conducir a los consumidores a medios de pago absolutamente atípicos. Destacan entre otros, la transferencia bancaria (muy inusual entre desconocidos), el envío de dinero o la utilización de cheques de caja, protagonistas de algunos de los tipos de fraude que se han analizado. El gráfico recoge el peso de estos medios de pago en 2006.

2.3 El *phishing*

2.3.1 Definición

Una de las características fundamentales del mundo electrónico actual es su velocidad de evolución. Los delincuentes han encontrado en la Red un camino perfecto para revitalizar, de forma más eficiente, las estafas tradicionales.

Esta rapidez de desarrollo también queda reflejada en la dificultad que supone proporcionar una única definición de qué se entiende por *phishing*, sobre todo, porque se trata de un fenómeno que se encuentra en permanente evolución.

Por lo que se refiere a la formación del término utilizado, el **Anti-Phishing Working Group –APWG-** (www.antiphishing.org) – organización de referencia en la lucha contra este delito

– explica que la palabra *phishing* procede de una analogía entre este delito y la pesca (en inglés: fish significa pescado). Así, los delincuentes utilizarían el correo electrónico como "cebo" para atrapar información confidencial de los destinatarios, en el "mar" que supone Internet.[17]

Otra definición, que contiene la idea básica que subyace tras el *phishing*, lo define como *"una forma de ingeniería social en la cual un atacante intenta de forma fraudulenta adquirir información confidencial de una víctima, haciéndose pasar por un tercero de confianza".* En efecto, no se trata de nada nuevo, la suplantación de entidades o personas con el objetivo de robar información personal de cualquier tipo para perpetrar fraudes ha sido utilizada fuera del mundo electrónico desde hace años. La diferencia respecto a la práctica moderna es, precisamente, el uso de la automatización y de los nuevos medios de comunicación, que han permitido desarrollar este tipo de delitos de forma masiva y en un corto periodo de tiempo.

Posiblemente la definición más citada es la que proporciona el APWG, y que ha sido ampliada en enero de 2007 para recoger las continuas mutaciones del fenómeno:

"Los ataques de phishing recurren a formas de ingeniería social y subterfugios técnicos para robar los datos de identificación personal de consumidores y las credenciales de cuentas financieras. Los ardides de ingeniería social se basan en correos electrónicos engañosos que conducen a los consumidores a sitios web falsos diseñados para estafar a los destinatarios para que divulguen datos financieros tales como números de tarjetas de crédito, nombres de usuario de cuentas, contraseñas y números de la seguridad social. Apropiándose de nombres comerciales de bancos, distribuidores y compañías de tarjetas de crédito, los phishers[18] a menudo convencen a los destinatarios para que respondan. Los subterfugios técnicos implican la instalación de crimeware[19] en ordenadores personales para robar las credenciales directamente, habitualmente utilizando troyanos[20] que captan las pulsaciones de teclado".

[17] El término fue acuñado en 1996 por los *hackers* que, en aquel entonces, robaban cuentas de usuario de América Online (AOL). La primera mención en Internet de la palabra *phishing* se produce en el famoso grupo de noticias "Alt.2600", en enero de ese mismo año. Respecto a por qué la "f" se transformó en "ph" hay diversas versiones en Internet. La historia que más se repite es que el término viene a rendir homenaje a la primera forma de *hacking* documentada: el "*phreaking*". Este delito consistía en el pirateo de los sistemas de telefonía con el objetivo final de no pagar por el servicio y el término fue popularizado por el primer *hacker* informático, John Draper. Desde entonces, una buena parte de los grupos dedicados a la piratería informática y de los pseudónimos que estos delincuentes adoptan en Internet incluyen esa "ph".

[18] Denominación empleada para designar a los estafadores que utilizan esta técnica.

[19] Conjunto de amenazas de Internet cuyo objetivo es la realización de delitos que permitan conseguir un beneficio económico, directa o indirectamente. http://www.pandasoftware.es/

[20] Los troyanos no se pueden considerar virus ya que no se replican o no hacen copias de si mismos. En realidad son programas que llegan a un ordenador de forma totalmente normal y no producen efectos realmente visibles o apreciables (por lo menos en ese momento). Pueden llegar acompañados de otros programas y se instalan en el ordenador del usuario. Al activarse pueden dejar huecos en nuestro sistema, a través de los cuales se producen intrusiones.

Esta definición ya recoge algunas de las "innovaciones" delictivas que han aparecido de forma más reciente, fundamentalmente en lo que se refiere al empleo de métodos basados en la tecnología. En concreto, focaliza en el correo electrónico el medio de dispersión utilizado. Si bien es cierto que el empleo de otros medios ha sido, en ocasiones, rebautizado (*smishing*, *vishing*, etc.), la esencia del engaño sigue siendo la misma.

En España, la **Asociación de Internautas -AI-** (www.internautas.org) también considera *phishing* a las prácticas de suplantación de identidad que utilizan medios distintos al correo electrónico, como son sitios web y llamadas o mensajes telefónicos.

A modo de resumen, de acuerdo con el documento publicado por el **Financial Services Technology Consortium -FSTC-** (www.fstc.org), lo que diferencia al *phishing* de otros tipos de fraude es que combina cuatro elementos fundamentales:

i) Ingeniería social: El *phishing* explota las debilidades de los individuos para engañarles y hacer que actúen contra sus propios intereses.

ii) Automatización: Las tecnologías de la información son utilizadas para desarrollar los ataques de *phishing* de forma masiva.

iii) Comunicación electrónica: Usan redes de comunicación, especialmente Internet.

iv) Suplantación: Un ataque de *phishing* requiere que los delincuentes suplanten a una empresa legítima o a una agencia gubernamental.

Partiendo de estas reflexiones y considerando las distintas fuentes involucradas de una u otra forma en el ámbito de los delitos informáticos, INTECO propone la siguiente **definición:**

"El *phishing es una forma de ataque basada en técnicas de ingeniería social, utilización de código malicioso o la combinación de ambas, en la que el delincuente, haciéndose pasar por alguna empresa o institución de confianza, y utilizando la tecnología de la información y las comunicaciones, trata de embaucar al atacado para que le proporcione información confidencial, que posteriormente es utilizada para la realización de algún tipo de fraude*".

2.3.2 Evolución del *phishing*.

Como se ha adelantado se trata de un fenómeno en permanente evolución que muta para adaptarse a diferentes situaciones.

Existen varios tipos de troyanos dependiendo de lo que hagan en el sistema: puerta trasera o "backdoors" (permite el acceso no autorizado al equipo), downloader (descarga otros códigos en la máquina), dialers (marcadores telefónicos), *Keyloggers* (captadores de pulsaciones), etc.

Los primeros casos de *phishing* surgen como un fraude de ingeniería social o "picaresca", en el que, suplantando la identidad de una organización conocida, y a través de un simple correo electrónico, se solicita una serie de datos al usuario. Normalmente se alega algún motivo de seguridad, o fallo en el sistema para requerirle esa información. El usuario responde el correo con sus datos personales, pensando que es el legítimo proveedor o entidad el que los solicita.

Poco a poco, el usuario va desconfiando de este tipo de correos, por lo que los ciberdelincuentes dan un paso más allá introduciendo un enlace a la supuesta web de la entidad, que en realidad se trata de una página fraudulenta, que imita la original, y que sirve para capturar los datos de usuario, contraseñas, etc. El perfeccionamiento de estas páginas ha sido progresivo. Se usan nombres parecidos a los originales e incluso idénticos pero con contenido falso que proviene de otro servidor. También se utilizan "ventanas emergentes" en los que no aparece ninguna dirección visible.

El siguiente paso del "*phishing*" es cambiar el canal de contacto, a través de "sms", llamado "***smishing***", o a través de voz IP. Se envía un correo electrónico, no invitando a visitar una web que puede crear desconfianza, sino para avisarle que será contactado vía "sms" o incluso telefonía IP, haciéndole creer que es un trabajador del banco que está revisando protocolos de seguridad.

De la misma manera han evolucionado los objetivos del *phishing* y los destinos de los ataques. Así, en un principio, se buscaban datos estrictamente bancarios (números de cuentas y de tarjetas de pago, claves de acceso, etc.) y se atacaban grandes grupos financieros.

A medida que en estos grandes grupos las medidas de seguridad informática van mejorando, se reorienta la acción del ciberdelincuente hacia entidades más pequeñas y, generalmente, menos protegidas, llegando por último a hacerse extensiva aquella actuación a todo tipo de proveedores con transacciones monetarias (agencias de viaje, portales de subastas, sistemas de pago, tiendas de comercio electrónico, webs de recarga de móviles, etc.) en busca de todo tipo de datos personales (direcciones, números de la Seguridad Social, números de teléfono, etc.).

La evolución más reciente del *phishing* enfoca el ataque hacia la personalización del ataque y la especialización de las técnicas.[21]

De un lado, aparecen nuevas variantes de *phishing* centradas en la personalización del ataque hacia colectivos concretos. El "***wishing***" o **"*whale phishing*"** dirige el ataque a individuos o pequeños grupos que cumplen con algún criterio determinado (altos

[21] http://seguinfo.*blog*spot.com/2007/06/hishing-y-wishing-nuevas-variantes-de.html; http://www.websense.com

funcionarios de gobierno, políticos, administradores de redes, etc.) El código es diseñado para estar "dormido", al acecho, y realizar análisis de sus comportamientos para robarles información.

Otra variedad de *phishing* es la denominada "***spear phishing***" ("pesca con arpón"). Se caracteriza por un trabajo de investigación previo por parte del *phisher*, permitiéndole el uso de cuentas de correo similares a las de personas de confianza o a las de entidades con las que la víctima tiene una relación real, ampliando así las posibilidades de éxito.

De otro lado, los ataques de *phishing* utilizarán nuevos métodos para distribuir *spyware* (programas espía) y malware (virus, troyanos, gusanos etc) informáticos. Ejemplos de esta evolución son: el "***hishing***" o ***"hardware phishing"*** que consiste en ocultar virus informáticos, *spyware*, *keyloggers*, troyanos, etc. en equipos que van a ser vendidos, ya sean estos nuevos o usados. Estos códigos maliciosos pueden ocultarse en teléfonos móviles, equipos MP3, etc. y; el "***blow phish***", que se trata de una combinación de criptografía con virus informáticos o códigos maliciosos. Se conocen también como cripto-virus.

2.3.3 Tipos de *phishing*.

Como hemos visto, han ido apareciendo en estos últimos años, diferentes tipos de *phishing*, aumentando su grado de sofisticación y profundidad.

La rapidez de evolución de este tipo de delitos complica también la tarea de realizar un análisis exhaustivo de todas las variantes que se pueden incluir bajo esta denominación común, más aún si tenemos en cuenta que, a menudo, se lanzan ataques combinados que implican el concurso de varias de las técnicas que pretendemos exponer.

Lógicamente, no existe una única clasificación de los delitos de *phishing*. Una de las más acertadas proporciona las distintas "fotografías" del modus operandi de estos delincuentes, describiendo seis tipos de *phishing*:[22]

1.- *Phishing* engañoso – Deceptive *Phishing*

Esta es la forma primitiva de *phishing*. Aunque en sus inicios (cuando el objetivo básico era la captura de cuentas de AOL) la herramienta de comunicación utilizada eran las aplicaciones de mensajería instantánea, en la actualidad la forma más habitual de desarrollar este tipo de delito (o al menos de iniciarlo) es mediante el correo electrónico. Precisamente, un típico ataque de esta variedad de *phishing* comienza cuando el *phisher* envía un correo electrónico falso.

[22] Jakobsson y Myers (2007)

El procedimiento es relativamente sencillo. Consiste, básicamente, en el envío, generalmente masivo, de un correo electrónico en el que es suplantada una empresa o institución legítima y de confianza para el receptor, por lo que este atendiendo una "llamada a la acción" incluida en dicha comunicación electrónica pulsará en el enlace contenido en el correo electrónico siendo desviado, de manera inconsciente, a un sitio web fraudulento.

Los ejemplos de llamada a la acción son muy diversos: desde la existencia de algún tipo de problema en la cuenta bancaria del destinatario, invitándole a entrar en algún sitio web para subsanarlo, la comunicación de algún tipo de riesgo por fraude, un aviso ficticio de compra acompañado de un enlace (link) cuyo destino es la página en la que puede cancelarse, la comunicación de un cambio no autorizado en la cuenta corriente del destinatario, etc.

En cualquiera de estos casos, el paso siguiente siempre es similar. Los destinatarios que son víctimas del engaño, acceden a un sitio web en el que se les requiere todo tipo de información confidencial para "subsanar" el problema que se les había comunicado previamente. Una vez recogidos esos datos, el *phisher* ya está en condiciones de realizar el fraude que previamente había planeado.

La variedad en este sentido también es muy amplia: desde la simple venta de esos datos para que otro realice el fraude a la transferencia de fondos de la cuenta bancaria del destinatario, la solicitud de una hipoteca en su nombre, la realización de compras por Internet, etc.

Dentro de esta tipología de *phishing* existen también distintas variantes. Una de ellas, relativamente común, es enviar mensajes de correo electrónico que, a través de HTML, replican con más o menos precisión la pantalla de autenticación de la entidad a la que están suplantando, evitando, de esta forma, que el usuario tenga que pulsar un link y utilizar el navegador web para realizar la acción. Mediante esta técnica se hace más difícil que el destinatario detecte el engaño.

No obstante, para evitar este último detalle que puede dar al traste con la estafa, los delincuentes utilizan distintas técnicas para ocultar la dirección web en la que están navegando atentos, en todo momento, a los objetivos del timo. Las técnicas comprenden desde el uso de la dirección IP numérica en lugar del nombre de dominio[23], al uso de pequeñas rutinas realizadas mediante lenguaje de programación (ej. en JavaScript) que esconden la barra de direcciones del navegador, pasando por el

[23] La dirección IP está formada por una serie numérica de cuatro grupos entre 0 y 255 separados por puntos y que identifica un ordenador conectado a Internet. Obviamente, este sistema no se utiliza para la navegación por las dificultades que supondría recordar esta serie de memoria. En su lugar, el DNS (Domain Name System o Sistema de Nombres de Dominio) traduce esos números a direcciones web, tal y como normalmente las utilizamos en los navegadores, que son fáciles de reconocer y recordar.

uso de lo que se denomina el “ataque de un dominio primo”, esto es, el registro de un nombre de dominio similar al de la organización a la que se está suplantando para realizar la estafa (por ejemplo, “www.entidadfinanci.era.es” en lugar de “www.entidadfinanciera.es”.

Otra variante dentro del ataque a través de correo electrónico consiste en mensajes tengan como finalidad la instalación de algún tipo de software malicioso. Este se ejecutaría en el ordenador del destinatario cuando este ingresa en el sitio web falso y confunda, de alguna forma, al usuario. No obstante, esta categoría entraría dentro del siguiente tipo de *phishing*, que se analizará seguidamente.

Conviene realizar un análisis más pormenorizado de la naturaleza de estos mensajes, con el objeto de identificar los rasgos que los caracterizan:

a) Suplantación de empresas con buena reputación para conseguir la necesaria confianza de sus víctimas.

   - Utilizan la imagen de la compañía (logotipo, colores, tipos de letra…).
   - Introducen enlaces al sitio web legítimo de la compañía junto al enlace fraudulento para confundir a los potenciales estafados.
   - El correo electrónico parece proceder de la compañía suplantada.

b) La dirección de respuesta es diferente de la identidad que hace el envío.

c) Crean un motivo plausible: la imaginación de los delincuentes es prolija, pero, básicamente, existen tres fuentes principales de estímulo:

   - el miedo (a ser objeto de un fraude)
   - la codicia (la posibilidad de aprovechar una buena oportunidad)
   - la curiosidad (acceder a algún contenido novedoso).

d) Requieren respuesta rápida: el fraude no puede prolongarse mucho tiempo.

e) Recolección de información vía correo electrónico (cada vez menos habitual).

f) Enlaces a dominios con nombres o grafías similares al del dominio legítimo.

g) El texto del enlace (link) en el correo electrónico difiere del enlace (link) de destino.

También es interesante analizar la segunda parte del engaño que, de forma más habitual, utiliza un sitio web como cebo. Las principales argucias utilizadas por este tipo de estafadores en los sitios web fraudulentos son:

a) En ocasiones los estafadores programan sus webs de tal forma que si el usuario utiliza un navegador que no tiene la vulnerabilidad que se pretende explotar, redireccionan al usuario a la web legítima, evitando ser descubiertos.

b) Camuflarse a la hora de suplantar la web legítima de la compañía. Incluso, muchos sitios web fraudulentos simulan el proceso de envío de los datos, tal y como sucedería en la versión legítima, y redireccionan al usuario a la página de la empresa suplantada una vez que los datos han sido facilitados. De esta manera las víctimas no saben que han sido objeto de un fraude.

c) Uso de certificados SSL falsos: una URL que comienza con el protocolo "https://", en lugar de "http://", indica que la información está siendo transmitida a través de una conexión segura y que la compañía está provista de un certificado Secure Sockets Layer (SSL). Algunos sitios web fraudulentos utilizan este protocolo y suele combinarse con la utilización de direcciones IP en lugar de la URL habitual. Curiosamente, los navegadores suelen desplegar mensajes en los que se avisa al usuario de que el certificado es inválido o que no coincide con el nombre del sitio. Sin embargo, la mayoría de usuarios suelen ignorar estos mensajes, pensando que es un error de su navegador y caen en la trampa.

d) Uso de una barra de dirección falsa, que puede contener la dirección legítima del sitio, pero sin ningún efecto sobre la web que se está visitando.

e) Uso de ventanas emergentes: el sitio fraudulento redirecciona al usuario a la web real de la institución suplantada y, simultáneamente, despliega una ventana, fraudulenta, que solicita y recoge los datos. Por ello, resulta de gran utilidad activar los bloqueadores de pop-ups que incorporan la mayoría de los navegadores actuales.

f) Deshabilita el botón derecho del ratón, el cual, despliega un menú que permite, entre otras cuestiones, verificar las propiedades de las web visitada.

g) Introducir mensajes para evitar que el usuario entre en la web suplantada, obteniendo así el tiempo suficiente para completar el fraude. Los delincuentes más avanzados tecnológicamente utilizan aplicaciones software para bloquear el acceso del usuario (al menos desde el ordenador infectado) al sistema.

Estos son algunos de los ardides más utilizados por estos estafadores. Sin embargo, continuamente aparecen nuevas herramientas orientadas a mejorar las tácticas de la estafa, así como nuevos y más imaginativos argumentos para confundir al usuario.

Como hemos podido comprobar este tipo de *phishing* basa su éxito fundamentalmente en las técnicas de ingeniería social, es decir, el papel del destinatario del fraude es fundamental: sin su "cooperación" no hay posibilidad de éxito.

Dentro de este primer tipo de *phishing* deben incluirse dos variantes que se diferencian por el medio de comunicación que es utilizado para iniciar la estafa: el *Vishing* y el *Smishing*.

El ***vishing*** utiliza el teléfono como herramienta. Se basa en el uso de un tipo de software denominado "war dialers" cuya función es realizar la marcación de teléfonos desde un ordenador, utilizando la tecnología de telefonía sobre IP. Una vez que el usuario atacado descuelga se activa una grabación que trata de convencerle o bien de que visite un sitio web para dar sus datos personales o bien de que directamente "confirme" sus datos en la misma llamada. El verdadero problema de este tipo de ataques es la confianza que la población tiene en el teléfono y en el uso que tradicionalmente han hecho de él las empresas legítimas.

El ***smishing***, del mismo modo, trata de embaucar a los usuarios, pero esta vez a través de mensajes de texto a móviles. El primer caso se dio en China: "*un ciudadano de Pekín, recibió un mensaje en su móvil informándole que el banco le había cargado la compra de objetos valorados en más de 2.000 euros. El mensaje adjuntaba un número de teléfono al que llamar. Una vez hecho, una voz grabada le pidió los datos de su cuenta. Horas después la habían vaciado*".[24]

Este *phishing* telefónico ya ha evolucionado desde ese primer caso. En estos momentos, el mensaje (SMS) que recibe la víctima le informa que alguien le ha dado de alta en algún servicio de pago para recibir, por ejemplo, determinados contenidos. Si la víctima desea darse de baja, deberá hacerlo a través de una web, en la cual una vez haya accedido, se le instalará un software de captura de datos.

El problema de esta técnica es que el envío de SMS resulta relativamente caro, lo que limita las posibilidades de actuación de los delincuentes, si bien es cierto que se han anunciado ya formas de conseguir, a través de *malware*, que sean otros los que corran con estos costes, lo que sin duda puede ser un indicio claro de su posible propagación.

2.- *Phishing* basado en software malicioso – *Malware*-Based *Phishing*

[24] ABC "El Semanal" 14/1/07

Con este tipo de *phishing* nos referimos de forma general a cualquier variante de este delito que implique la ejecución de un software malicioso en el ordenador de la víctima.

La propagación de este tipo de *phishing* puede depender tanto de las técnicas de ingeniería social como de la explotación de una vulnerabilidad del sistema. En el primero de los casos, el ataque debe conseguir, como paso previo, que el usuario realice alguna acción que permita la ejecución del *malware* en su máquina: abrir el archivo adjunto de un correo electrónico, visitar una web y descargar el programa. Las técnicas sociales para conseguir que el usuario actúe de este modo son, al igual que en el caso anterior, muy diversas, si bien este método suele inclinarse más por la promesa de algún contenido llamativo para el destinatario.

En lo que se refiere a la explotación de vulnerabilidades del sistema, la amenaza es mucho más difícil de combatir, ya que existen variantes en las que la actuación del usuario es mucho menor. Así, aunque muchas de las estafas se basan en que sea el usuario el que, de una u otra manera, introduzca la aplicación en su máquina, también es posible que los delincuentes aprovechen fallos en la seguridad del sistema de un sitio web legítimo para introducir software malicioso que les permita llevar a cabo su objetivo.

Con independencia de cuál sea la técnica empleada para conseguir la ejecución del código malicioso en el ordenador personal del atacado, podemos distinguir distintos tipos de programas diseñados para robar datos confidenciales:

- *Keyloggers* y Screenloggers. Los *keyloggers* son programas cuya función es el registro de las pulsaciones que se realizan en el teclado. La aplicación en el ámbito del *phishing* es evidente: estas aplicaciones suelen estar programadas para ponerse en funcionamiento cuando la máquina en la que están instaladas accede a alguna web registrada por el programa (entidad financiera, subasta online). En ese momento, graba todo lo que se teclea en el ordenador y, posteriormente, lo envía al delincuente que de esta forma consigue su propósito de robar información confidencial.

  Existen versiones más avanzadas que también capturan los movimientos de ratón. Algunas entidades, conscientes de la existencia de este tipo de programas y de su posible aplicación delictiva han introducido contramedidas como la disposición de teclados en pantalla para evitar las pulsaciones de teclado en la introducción de contraseñas.

  Los *screenloggers* realizan la misma función pero, en lugar de capturar pulsaciones de teclado, capturan imágenes de la pantalla que son remitidos al atacante.

- Secuestradores de sesión (Session Hijackers). Este tipo de aplicaciones operan una vez que el usuario ha accedido a alguna web registrada por el software, esto es, no roba datos, sino que directamente actúa cuando la victima ya ha accedido a su cuenta corriente su sesión en una subasta. Estos programas suelen ir "disfrazados" como un componente del propio navegador. Esta forma de *phishing* puede realizarse tanto mediante la instalación del *malware* en el ordenador del destinatario de la estafa, como mediante la técnica del "man in the middle" o intermediario.[25]

- Troyanos web (web Trojans). Son programas maliciosos que aparecen inesperadamente, en forma de ventanas emergentes, sobre las pantallas de validación de páginas web legítimas, con el objetivo de conseguir datos confidenciales. En este caso, la finalidad que persiguen es hacer creer al usuario que está introduciendo la información en el sitio web real, cuando en realidad lo que está haciendo es introducirlo en este software que, posteriormente, remite los datos al delincuente, con las consabidas consecuencias. El *phishing* parece la aplicación "natural" de este tipo de programas fraudulentos.

- Ataques de reconfiguración de sistema (System Reconfiguration Attacks). Este tipo de ataques se efectúan a través de la modificación de los parámetros de configuración del ordenador del usuario. Existen diversas formas de realizar estas acciones. Una de ellas consiste en modificar el sistema de nombres de dominio, tal como se explicaba en el caso anterior. Otra posibilidad al alcance de los delincuentes es la instalación de lo que se denomina un "proxy", a través del cuál se canalice toda la información que sale y entra de la máquina del usuario. Esta forma de ataque se corresponde también con la técnica del "man in the middle" (MitM).

- Robo de datos (Data Theft). También existen códigos maliciosos cuya finalidad consiste en recabar información confidencial almacenada dentro de la máquina en la que se instalan y remitirla al delincuente (direcciones, números de identidad, claves).

3.- *Phishing* basado en el DNS o "*Pharming*" (DNS-Based *Phishing*)

Dentro de esta rúbrica se incluyen todas aquellas formas de *phishing* que se basan en la interferencia del proceso de búsqueda del nombre de dominio (la traducción de la dirección introducida en el navegador a la dirección IP). Sin duda, el *pharming*, denominación habitual de esta forma de llevar a cabo este tipo de delito, supone un

[25] Ataque en el que el delincuente es capaz de leer, insertar o modificar a voluntad los mensajes entre 2 partes sin que ninguna de ellos conozca que el canal entre ellas ha sido violado.

peligro aún mayor que algunas de las otras variantes que se han analizado, ya que la colaboración de la víctima es menor y, además, el disfraz empleado por los delincuentes parece más real.

Como se señalaba al hablar de ciertos tipos de código malicioso, cuando un usuario navega por la Red recurre a la utilización de direcciones URL, relativamente fáciles de recordar (por ejemplo, www.inteco.es). Sin embargo, estas direcciones tienen que ser traducidas a lo que se denominan direcciones IP. Esa traducción se realiza, en los sistemas operativos de diversas formas. Por un lado, existen los denominados Servidores de Nombres de Dominio (Domain Name Server o DNS) que cumplen explícitamente esta función. Cuando un usuario desea acceder a un sitio web envía una petición a uno de estos servidores que transforman la URL introducida en la barra de direcciones del navegador en la dirección IP. El proceso es transparente para el usuario.

Otra forma de llevar a cabo esa transformación es mediante el fichero hosts. Este fichero -incluido en el sistema operativo, almacena la información de las páginas que el usuario ya ha visitado- con el fin de evitar la consulta al servidor DNS y acelerar el proceso. Además, en esta misma línea, la memoria caché del navegador también conserva información de las webs visitadas, siempre con el fin de reducir el tiempo de respuesta para la navegación.

4.- *Phishing* mediante introducción de contenidos (Content-Injection *Phishing*).

Esta modalidad consiste en introducir contenido malicioso dentro de un sitio web legítimo. Dicho contenido puede tener diversas modalidades: redirigir a los visitantes a otra página, instalar algún tipo de *malware* en el ordenador de los usuarios, etc. Básicamente, existen tres categorías principales de *phishing* mediante introducción de contenidos, a partir de las cuales surgen un número indefinido de variantes:

- Asalto al servidor legítimo por parte de *hackers* que se aprovechen de una vulnerabilidad para modificar o introducir contenido malicioso en el sitio web.

- Introducción de contenido malicioso en el sitio a través de lo que se denomina una vulnerabilidad de “cross-site scripting”, también conocido como XSS. El cross-site scripting es una vulnerabilidad que aprovecha la falta de mecanismos de filtrado en los campos de entrada y permiten el ingreso y envío de datos sin validación alguna, aceptando el envió de scripts completos, pudiendo generar secuencias de comandos maliciosas que impacten directamente en el sitio o en el equipo de un

usuario[26]. Este tipo de vulnerabilidad puede afectar tanto a la aplicación web como a los usuarios que activen esa secuencia de comandos de forma involuntaria.

- Acciones maliciosas que pueden ser llevadas a cabo en un sitio a través de una vulnerabilidad de introducción de SQL (SQL injection vulnerability). Esta es una forma de provocar que sean ejecutados comandos de bases de datos en un servidor remoto que conlleven la filtración de datos confidenciales. Al igual que en el caso anterior, esta vulnerabilidad se debe a la ausencia de filtros adecuados en el servidor que impiden dicha ejecución.

5.- *Phishing* mediante la técnica del intermediario (Man-in-the-middle *Phishing* o MitM)

Aunque en muchas de las clasificaciones consultadas se considera ésta como una categoría dentro de los tipos de *phishing*, en realidad se trata de una técnica para efectuar el ataque. Como su propia denominación indica, implica el posicionamiento del *phisher* entre el ordenador del usuario y el servidor web legítimo. De este modo el delincuente se hace con la capacidad de filtrar, leer, e incluso modificar la información que se transfiere desde el puesto del atacado al servidor y viceversa, sin que las partes sean conscientes de la violación de su seguridad. Las consecuencias de esta actuación pueden ser tanto el robo de información confidencial, para su uso o venta posterior, o, directamente, el secuestro de la sesión (*session hijacking*), en cuyo caso podrá o no robar esa información. Nuevamente, el problema de esta variante es que el usuario no puede detectar que está siendo víctima de un delito ya que, aparentemente, todo funciona de forma correcta.

La utilización de esta técnica para desarrollar distintos tipos de *phishing* admite diferentes modalidades. Ya se comentaron los ataques tipo *proxy*, que son los que más habitualmente se realizan a través de este procedimiento. Sin embargo otras variedades pueden llevarse a cabo utilizando tipos como el ataque basado en DNS y basado en el engaño, categorías también analizadas con anterioridad.

6.- *Phishing* de motor de búsqueda (Search Engine *Phishing*)

Nuevamente más que un tipo de *phishing* es, en sí mismo, uno de los ardides empleados por los delincuentes para hacer que el usuario caiga en su trampa. Los delincuentes crean páginas web para productos o servicios falsos, las introducen en los índices de los motores de búsqueda y esperan a que los usuarios visiten las páginas para realizar compras y, por tanto, proporcionen información confidencial o directamente realicen transferencias bancarias. Normalmente las falsas ofertas tienen

[26] Definición extraída de http://www.desarrolloweb.com.

condiciones sensiblemente mejores a las ofrecidas por empresas legítimas, con el objetivo de atraer al máximo número de víctimas posible.

En este ámbito han tenido mucho éxito los fraudes en los que los *phishers* se han hecho pasar por bancos que ofrecen tipos de interés muy superiores a los ofrecidos por las entidades financieras reales. Las víctimas encuentran estos falsos bancos online a través de buscadores y, ante tal oferta, no dudan en abrir una nueva cuenta e introducir sus datos bancarios para realizar una transferencia.

La clasificación presentada (como se reconoce en su introducción y como se ha ido mostrando en su descripción), adolece de algunos defectos, entre los que destaca la falta de criterio de distinción entre unos tipos de delito y otros, y la existencia de zonas comunes entre las categorías consideradas. Sin embargo, también se ha de reconocer una virtud importante: la descripción prácticamente exhaustiva de variantes de *phishing*.

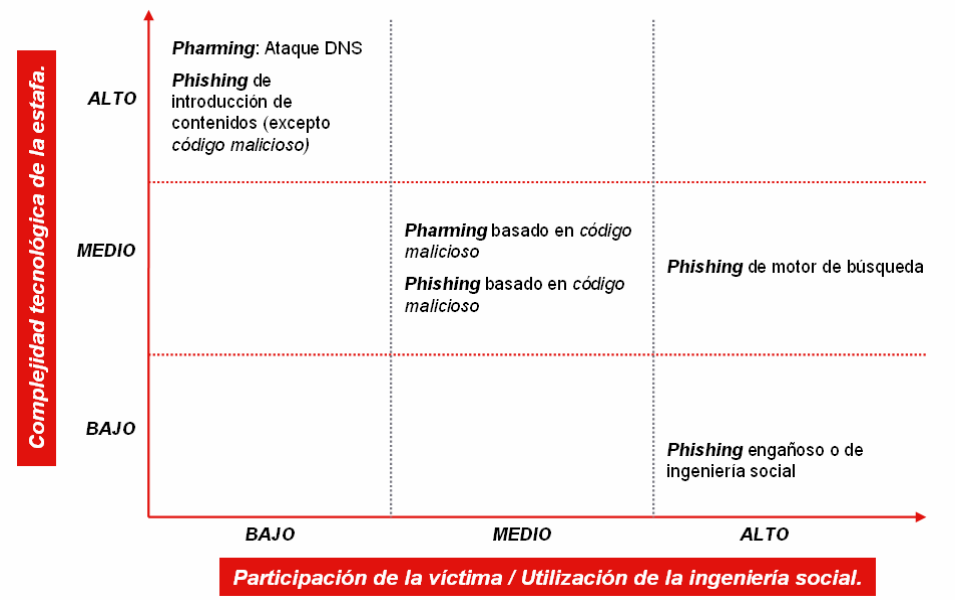
Con el objetivo de arrojar algo de luz, se incluye su reclasificación tratando de eliminar estas debilidades, para ofrecer una visión más rigurosa del tipo de problemas al que los usuarios se enfrentan y, sobre todo, proponiendo criterios útiles en el ámbito de la propuesta de medidas para atajar estas actividades. De este modo, se proponen dos clasificaciones, en función de:

- Nivel de participación de la víctima.
- Complejidad tecnológica de la estafa.

Partiendo de esta idea, se señala la clasificación que aparece en el esquema, distinguiendo tres niveles de colaboración por parte del usuario: alto, medio y bajo. Si se quiere, esta tipología puede proponerse desde el punto de vista contrario, esto es, cuál es el nivel de ardides de ingeniería social que debe utilizar el delincuente para llevar a cabo el fraude.

En lo que se refiere a la complejidad tecnológica, lógicamente, cuanto mayor es ésta menos necesaria es la participación de la víctima para llevar a cabo la estafa. Así, encontramos una relación directa entre ambos criterios, reflejada en la Gráfico 7.

Gráfico 7: Clasificación del *phishing* según la participación de la víctima y la complejidad tecnológica de la estafa



Fuente: INTECO

Se observa cómo la mayor parte de los casos se encuentran en los cuadrantes que formarían la diagonal secundaria del esquema, esto es, las combinaciones inversas entre los dos factores considerados y el punto intermedio tanto de complejidad tecnológica como de "colaboración" del estafado. Sólo hay un caso que se considera que se aleja de esta pauta: el *phishing* de motor de búsqueda. En este caso, la implicación del usuario es relativamente alta.

2.3.4 Fases del *phishing*

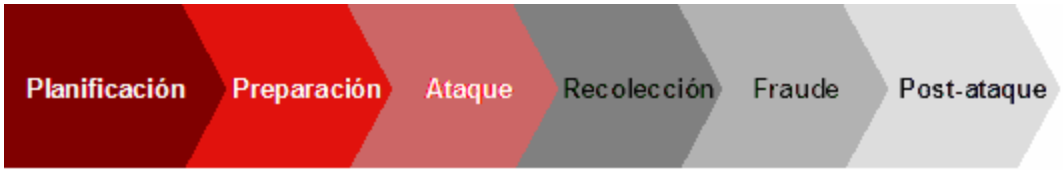
Diversas investigaciones han observado la existencia de un conjunto de pautas más o menos estable en los ataques realizados por este tipo de delincuentes. El análisis de estas etapas puede constituir una valiosa información en la lucha contra los *phishers*.[27]

La existencia de distintas variantes de esta estafa implica que, en muchas ocasiones, las fases pueden cambiar en cuanto a su profundidad, extensión y dificultad, al igual que respecto a los agentes que deben intervenir y cuál es el papel que deben jugar.

Seis son las fases principales que se completan en todo ataque de *phishing* (Gráfico 8):

[27] Se propone un esquema de acción de los *phishers*, partiendo de los análisis realizados por la FSTC (Financial Services Technology Consortium) en 2005, la NCL (National Consumer League) en 2006 y el informe realizado por Emigh (2006) al amparo de diversas instituciones entre las que destaca el Anti-Phishing Working Group.

Gráfico 8: Fases del *phishing*



Fuente: INTECO

Fase de planificación

Durante esta etapa, el *phisher* toma las principales decisiones que va a llevar a cabo: a quién va dirigido el ataque, cómo y dónde se va a realizar, qué tipo de argucia se va a utilizar, cuál es el objetivo del fraude, qué medios necesitará para hacerlo, etc. Obviamente, esta etapa es común a cualquiera de los tipos de *phishing* analizados.

Se puede hacer una división de las tareas que se llevan a cabo en este primer estadio del fraude y reflexionar sobre quiénes son los implicados y cuál es su papel, teniendo en cuenta la clasificación de los tipos de *phishing* que se propuso con anterioridad, según el contenido tecnológico y el nivel necesario de participación de la víctima.

En la Tabla 3 se distinguen quiénes son los principales implicados en la realización de las tareas y qué tareas han de desarrollarse. En este sentido se diferencian entre tareas comunes a los tres tipos de *phishing* y actividades específicas.

Una de las primeras cuestiones que se plantea un *phisher*, cualquiera que sea la modalidad de estafa elegida, es tomar la decisión de realizar el ataque de forma colectiva o en solitario.

Sea cual fuera la opción elegida, otra decisión tomada por el delincuente en esta fase es qué tipo de datos se desean conseguir: información de cuentas bancarias, nombres de usuario y contraseñas, datos personales de diversa índole, etc. Esta cuestión estará vinculada a cuál es el tipo de fraude que se intenta cometer.

Tomadas estas decisiones, entramos en las cuestiones específicas, dependientes del tipo de *phishing*. Así, cuando el tipo de delito elegido entra en la categoría de “alta complejidad tecnológica” y “baja participación de la víctima”, la elección fundamental es cuál será la empresa o institución atacada y a través de qué debilidad. En este caso, las víctimas finales, los usuarios, no tienen una implicación directa en esta fase, ya que el ataque no se llevará a cabo en sus ordenadores. Una vez seleccionado el objetivo, el delincuente planifica los medios y cómo conseguirlos.

Tabla 3: Fase de Planificación del delito

	Agentes	Tareas
Alta complejidad **Baja participación**	*Phisher* y colaboradores	**Selección de objetivo:** • Empresa o institución a atacar **Selección del método:** • Ataque al servidor DNS, búsqueda de vulnerabilidad,… o ¿Qué "materiales" son necesarios? o ¿Cómo los consigo?
Media complejidad **Media/Alta participación**	*Phisher* y colaboradores	**Selección de objetivo:** • ¿Quién es la víctima? • ¿Cómo la localizo? • ¿A qué empresa o institución suplanto? (si es necesario) **Selección del método:** • Tipo de *malware* • Forma de ataque (web, correo electrónico,…) • ¿Qué técnicas de ingeniería social se usarán? • ¿Qué "materiales" son necesarios? • ¿Cómo los consigo?
Baja complejidad **Alta participación**	*Phisher* y colaboradores	**Selección de objetivo:** • ¿Quién es la víctima? • ¿Cómo la localizo? • ¿A qué empresa o institución suplanto? (si es necesario) **Selección del método:** • Forma de ataque (web, correo electrónico,…) • ¿Qué técnicas de ingeniería social se usarán? • ¿Qué "materiales" son necesarios? • ¿Cómo los consigo?

Fuente: INTECO

En los ataques del tipo "complejidad tecnológica media" y "participación de la víctima media/alta" (se incluye la tipología de *phishing* de motor de búsqueda) cobra interés la determinación de la víctima, ya que implican en la mayoría de los casos la instalación de *malware* en sus ordenadores personales. Aquí, la planificación puede ser muy variable: desde la aceptación de una base de direcciones electrónicas conseguidas al azar, hasta el *spear phishing*, que puede conllevar el estudio pormenorizado del perfil de las víctimas, pasando por todas las posibilidades existentes entre ambos extremos.

También es relevante determinar la institución o empresa a suplantar, ya que muchas de las estafas implican que el delincuente se haga pasar por una entidad en la que la víctima tenga confianza.

Como se observa en la tabla, estas tareas son comunes con las estafas de “complejidad tecnológica baja” y “participación de la víctima alta” al igual que algunas cuestiones relativas a la selección del método: qué forma de ataque se empleará (cómo se comunicará con las víctimas), qué artimañas de ingeniería social se emplearán o qué medios serán necesarios aunque estas dos últimas cuestiones suelen tener respuestas muy diferentes en función del tipo de delito. De hecho, los materiales necesarios en la tipología media incluyen siempre algún tipo de código malicioso.

Fase de preparación

Si bien, en general, no existen grandes diferencias entre los tres tipos de *phishing* (Tabla 4), estas sí pueden apreciarse cuando se analizan tareas de creación y consecución de cada uno de ellos.

Los delincuentes deben conseguir el software, los datos de contacto, localizar los destinos de sus ataques, preparar sus equipos, construir los sitios web diseñados para efectuar el fraude y otras tareas, teniendo en cuenta las necesidades de cada tipo de delito que sí son diferentes, tal y como se apuntó al describir la fase de planificación.

En ocasiones, los delincuentes realizan ataques muy localizados dirigidos a personas u organizaciones muy concretas, lo que requiere el envío de correos mucho más elaborados que los que se utilizan en envíos masivos. Lo interesante de este tipo de ataques es su estudiada segmentación en la búsqueda de objetivos y preparación del engaño.

Un ejemplo de ello, es el intento de infección por correo electrónico que engañó a 1.400 directivos de importantes empresas mediante una supuesta carta de la **Better Business Bureau –BBB-** (www.bbb.org) perfectamente personalizada y redactada, que instaba a la ejecución de un programa que no era más que un troyano bancario.

Otros ejemplos de ataques muy elaborados han sido los recientemente dirigidos contra instituciones públicas de nuestro país. Así, en enero de 2007 se produjeron dos suplantaciones ilícitas de dos organismos de carácter nacional, si bien fueron rápidamente descubiertos y los usuarios de dichos servicios fueron alertados. Tomando como ejemplo uno de los casos, las posibles víctimas del engaño recibían un correo electrónico en el que figura el logotipo de la Agencia Tributaria, y en el que se comunicaba al destinatario que tenía una devolución tributaria pendiente. El mensaje decía que para poder recibirla se debía acceder a una página web (falsa) que imitaba perfectamente el diseño de la original para mantener la confianza de los contribuyentes destinatarios, a los que se solicitaba que rellenasen un formulario en el que debían figurar los datos de su tarjeta de crédito.[28]

[28] Un nuevo intento de estafa usa a Hacienda como reclamo.
http://www.elpais.com/articulo/internet/nuevo/intento/estafa/usa/Hacienda/reclamo/elpeputec/20070130elpepunet_11/Tes

Cada vez con mayor frecuencia, se observa este tipo de estafas más elaboradas, que requieren de un trabajo de campo previo y huyen de las reglas habituales del *spam* masivo, impersonal y poco sofisticado. Así, los estafadores en la fase de preparación harán sus cábalas y estimarán sus costes y beneficios entre elegir un ataque más o menos complejo (envío masivo frente al personalizado, traducción automática frente a textos cuidados, etc).

Tabla 4: Fase de preparación del ataque

	Agentes	Tareas
Alta complejidad Baja participación	*Phisher* y colaboradores	Creación/consecución de medios
Media complejidad Media/Alta participación	*Phisher* y colaboradores	Creación/consecución de medios
Baja complejidad Alta participación	*Phisher* y colaboradores	Creación/consecución de medios

Fuente: INTECO

Fase de ataque

En este momento, las estafas que implican una participación "media" o "alta" de las víctimas requieren de su concurso, ya que acciones como abrir un correo electrónico, visitar una página web o realizar una búsqueda, son acciones necesarias para que el ataque se consuma (Tabla 5).

Una estafa de 'phishing' suplanta la imagen del INE para robar datos de usuarios. http://www.20minutos.es/noticia/195851/0/phishing/ine/estafa/

Tabla 5: Fase de ataque

	Agentes	Tareas
Alta complejidad Baja participación	• *Phisher* y colaboradores • Empresa/Institución	• Ataque al servidor DNS o al servidor de la empresa o institución
Media complejidad Media/Alta participación	• *Phisher* y colaboradores • Víctima	• Comunicación con la víctima (lanzamiento del "cebo"): o Correo electrónico (con o sin adjunto) o Mensajería instantánea o SMS o VoIP o P2P • Puesta en funcionamiento de la web para distribuir el ataque con *malware* (en caso de no utilizar correo electrónico directamente) • Registro de la web falsa en motores de búsqueda (caso del *Phishing* de motor de búsqueda)
Baja complejidad Alta participación	• *Phisher* y colaboradores • Víctima	• Comunicación con la víctima (lanzamiento del "cebo"): o Correo electrónico (con o sin formulario) o Mensajería instantánea o SMS o VoIP • Puesta en funcionamiento de la web para recoger datos (en caso de no utilizar correo electrónico directamente)

Fuente: INTECO

En lo que se refiere a las tareas, no hay tareas comunes, ya que dependen del tipo de *phishing* seleccionado. Así, en el primer caso el ataque se centra en el servidor de la empresa o institución objetivo, mientras que en los otros dos tipos se trata de comunicar o preparar las trampas para las víctimas, utilizando distintos medios.

A este respecto es especialmente interesante detenerse en los ataques a través de *malware*. En este sentido en el Gráfico 9 se observa dónde se lleva a cabo exactamente la infección y cuál es el punto en el que los datos confidenciales se comprometen. Este esquema, que representa lo que se denomina "anatomía de un ataque de *phishing*",[29] localiza siete elementos fundamentales: el *malware*, la infección, la ejecución, el almacenamiento, la entrada de datos, el atacante y el servidor legítimo.

[29] Emig (2006)

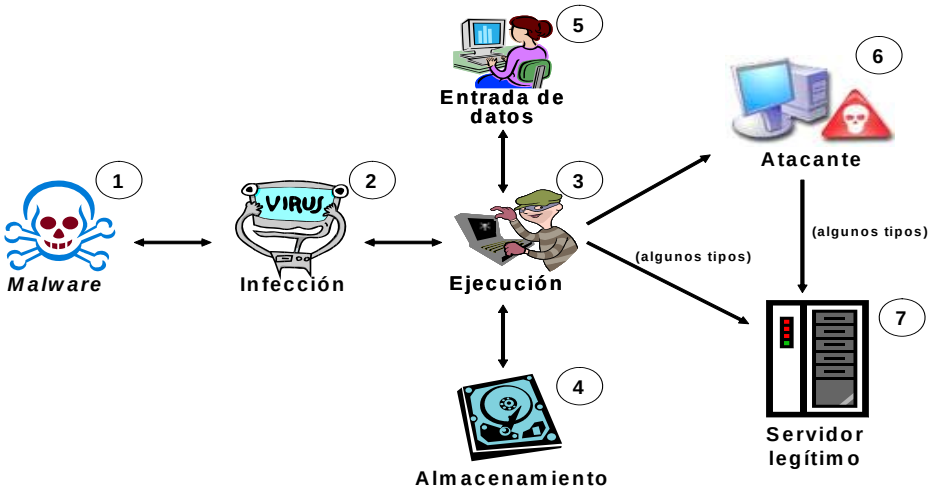
Como se observa en la siguiente gráfico los puntos de infección en este tipo de ataques son: bien el momento de la propia infección (esto es, cuando entra en el sistema el *malware*, no siendo necesaria su ejecución), o bien en el momento en que se ejecuta el código malicioso. Respecto a la consecución del objetivo por parte del atacante, esto es, la captación de información confidencial, también difiere en ubicación en función del tipo de aplicación utilizada:

- Ataques en los que el propio *phisher* se apropia de la información por la fuerza (secuestradores de sesión, troyanos web y reconfiguración de sistema a través de *proxy*).

- Ataques en los que el código malicioso recopila la información dentro de los dispositivos de almacenamiento de la máquina infectada.

- Situaciones en las que es el usuario, de forma involuntaria, quien proporciona la información (*keyloggers/screenlogger* y envenenamiento del fichero *hosts*).

Gráfico 9: "Anatomía" del *phishing*



Código malicioso	Punto de infección	Punto de compromiso de datos
Captador de pulsaciones/Grabador pantalla	Momento 2	Momento 5
Secuestrador de sesión	Momento 2	Momento 6
Troyano web	Momento 2	Momento 6
Envenenamiento de fichero *hosts*	Momento 3	Momento 5
Reconfigurador de sistema: Proxy	Momento 3	Momento 6
Robo de datos	Momento 3	Momento 4

Fuente: INTECO

Fase de recogida de datos

La fase de recogida de datos (Tabla 6) se anticipó esta fase en la descripción de la etapa anterior para el tipo de delito que implica niveles medios de complejidad y "colaboración". Los otros dos tipos restantes implican la espera de víctimas que entren en el servidor atacado, que respondan al mensaje enviado o que visiten la web fraudulenta. Adicionalmente, en el caso de ataque a un servidor, normalmente una vez instalado el código en la fase anterior es necesaria su ejecución para conseguir los datos, tarea más propia de esta fase.

Tabla 6: Fase de recogida de datos

	Agentes	Tareas
Alta complejidad Baja participación	• *Phisher* y colaboradores • Empresa atacada • Víctimas	• A la espera de los datos • Ejecución de código malicioso
Media complejidad Media/Alta participación	• *Phisher* y colaboradores • Víctimas • Empresa suplantada (si existe)	• A la espera de datos (aplicaciones autónomas y *Phishing* de motor de búsqueda) • Ejecución de códigos maliciosos para la consecución de datos (robo de datos, *pharming*)
Baja complejidad Alta participación	• *Phisher* y colaboradores • Víctimas • Empresa suplantada	• A la espera de datos (vía respuesta correo electrónico o visita a la web fraudulenta)

Fuente: INTECO

Fase de ejecución del fraude

Una vez recogidos los datos, el siguiente paso efectuado por los delincuentes es la realización de la estafa, bien de forma directa o bien vendiendo los datos robados para que otros estafadores consuman el delito.

En la Tabla 7 se recogen, como en casos anteriores, los implicados y las tareas que, en este caso, son comunes a los tres tipos de delito, con alguna excepción. La variedad en esta ocasión dependerá de los datos apropiados ilegalmente.

Tabla 7: Fase de ejecución del fraude

	Agentes	Tareas
Alta complejidad Baja participación	• *Phisher* y colaboradores • Empresa atacada • Víctimas • Otras empresas (si es el caso)	• Utilización o venta de los datos para realizar fraudes
Media complejidad Media/Alta participación	• *Phisher* y colaboradores • Víctimas • Empresa suplantada (si existe) • Otras empresas (si es el caso)	• Utilización o venta de los datos para realizar fraudes • Utilización de las sesiones secuestradas • Recepción directa de transferencias
Baja complejidad Alta participación	• *Phisher* y colaboradores • Víctimas • Empresa suplantada • Otras empresas	• Utilización o venta de los datos para realizar fraudes

Fuente: INTECO

Fase de post-ataque

La última fase, denominada de post-ataque (Tabla 8), tendría para el delincuente la finalidad de eliminar las pistas que hayan quedado. En este sentido, todos los implicados en el ataque pueden ser susceptibles de participar (activa o pasivamente) en el proceso, mientras que las tareas serán específicas de cada tipo de delito.

Lógicamente, además de las actividades propias de estos delitos, los estafadores procederán al blanqueo de los beneficios obtenidos de la operación y otros procesos normales en cualquier tipo de robo o fraude.

Tabla 8: Fase de post-ataque

	Agentes	Tareas
Alta complejidad Baja "colaboración"	• *Phisher* y colaboradores • Empresa atacada • Víctimas • Otras empresas (si es el caso)	• Eliminación del código malicioso • Eliminación de posibles rastros electrónicos
Media complejidad Media/Alta "colaboración"	• *Phisher* y colaboradores • Víctimas • Empresa suplantada (si existe) • Otras empresas (si es el caso)	• Eliminación del código malicioso • Eliminación de webs fraudulentas • Eliminación de registros en motores de búsqueda • Eliminación de posibles rastros electrónicos
Baja complejidad Alta "colaboración"	• *Phisher* y colaboradores • Víctimas • Empresa suplantada • Otras empresas	• Eliminación de direcciones de correo electrónico falsas • Eliminación de páginas web fraudulentas • Eliminación de posibles rastros electrónicos

Fuente: INTECO

2.4 El *phishing* en cifras.

El Estudio describe hasta el momento, desde un plano eminentemente teórico, las distintas facetas que caracterizan el fraude a través de la Internet, en general, y el *phishing*, en particular.

A continuación se recoge la presentación de datos para ofrecer una medida aproximada de la magnitud del fenómeno desde el panorama nacional e internacional. La información recogida de ambos escenarios se estructura en forma similar y homogénea.

Conviene, antes de comenzar con la descripción de esta información estadística apuntar las siguientes consideraciones:

- La primera consideración es que existe cierta **escasez de datos** (salvando el caso de EEUU, para el que se dispone de un mayor número de estadísticas) y se detecta cierta dispersión en lo que a estos se refiere.

- La mayoría de las estadísticas disponibles son las publicadas por distintas empresas dedicadas a la seguridad informática, por lo que **las muestras se circunscriben a los casos de sus propios clientes, limitándose la representatividad** cuantitativa, por lo que se deben tomar precauciones a la hora de su interpretación.

2.4.1 El panorama internacional del *phishing*.

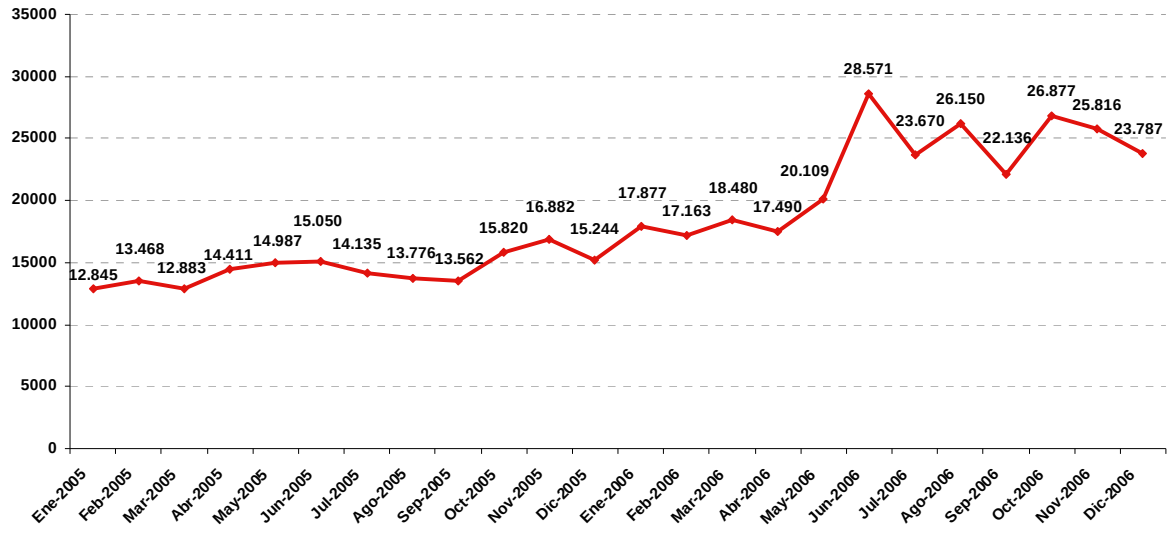
A nivel internacional, la fuente de datos más reconocida es el **Anti-Phishing Working Group -APWG-** (www.antiphishing.org) que además de apoyar la realización de investigaciones puntuales, realiza una serie de informes mensuales que tienen como objetivo la realización de fotos fijas sobre la incidencia del *phishing* y otros delitos relacionados (*pharming* y otras variantes).

Desde el plano institucional, destaca la labor realizada por la Organización **para la Cooperación y el Desarrollo Económico –OCDE-** (www.oecd.org) y los datos recogidos por **Eurostat** (www.eurostat.com) que, si bien no se refieren de forma específica al *phishing*, sí ofrecen medidas relacionadas que pueden ofrecer indicios sobre determinadas cuestiones afines. También hay diversas iniciativas en desarrollo en la **Comisión Europea** (http://www.europa.eu/scadplus/leg/es/lvb/l33193b.htm) cuyo objetivo es el estudio de aspectos relacionados con delitos informáticos.

A continuación, se recoge un conjunto de las principales variables utilizadas por las fuentes de datos anteriormente señaladas. Destacan entre dichas variables: el número de ataques de *phishing*, el número de sitios web orientados a realizar el *phishing*, el número de marcas suplantadas, el origen de procedencia de los ataques, los sectores más afectados, los periodos de tiempo más activos, las técnicas empleadas y la utilización de código malicioso para la creación del fraude.

La forma más habitual de medir la evolución del fraude, empleada tanto por el APWG, como por otras fuentes de información es el **número de ataques únicos de *phishing*** (Gráfico 10) o “campañas de e-mail”, esto es, un único correo electrónico enviado a múltiples usuarios y cuyo objetivo es redireccionarlos a un único website fraudulento.

Gráfico 10: Número de ataques únicos de *phishing*



Fuente: APWG

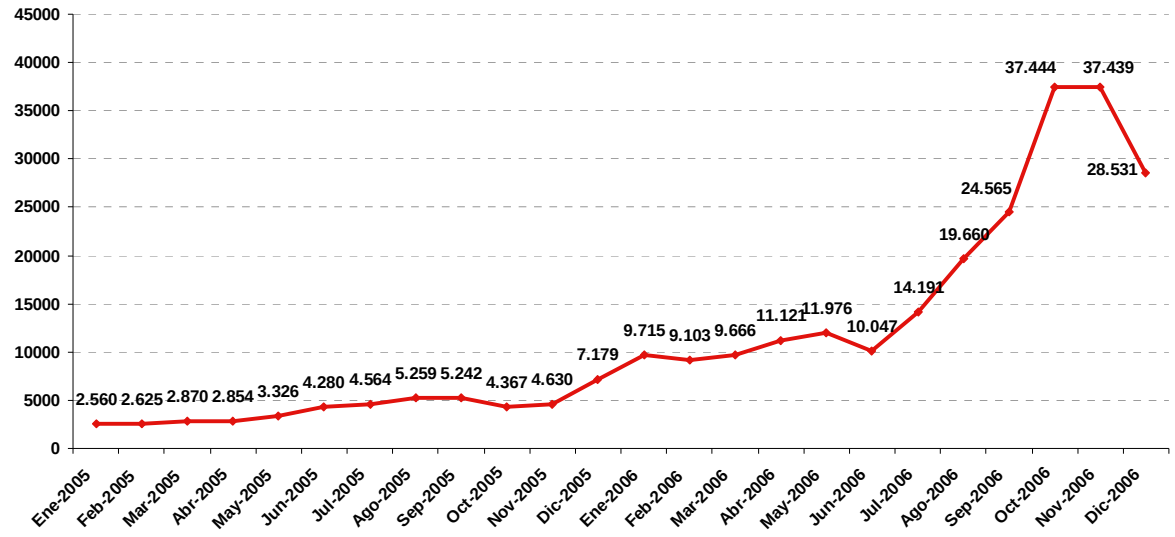
Entre enero de 2005 y diciembre de 2006 el número de ataques únicos se ha duplicado, superando a finales del pasado año los 20.000 ataques mensuales. Esta tendencia implica que en el año 2007 se superarán los 250.000 ataques únicos.

Este crecimiento puede explicarse por el desarrollo de herramientas orientadas a facilitar la actividad de los delincuentes y el cambio de motivación de estos.[30]

Esta tendencia se confirma al analizar otras medidas como el **número de sitios web orientados a realizar el fraude** (Gráfico 11).

[30] INTECO analizó en la Primera oleada del "Estudio sobre la Seguridad de la Información y eConfianza en los hogares españoles" este cambio de filosofía en la forma de actuar de los desarrolladores de *malware*, que han pasado actuar en busca de notoriedad a tener una motivación en sus actos puramente económica.

Gráfico 11: Número de sitios web fraudulentos para la realización de *phishing*



Fuente: APWG

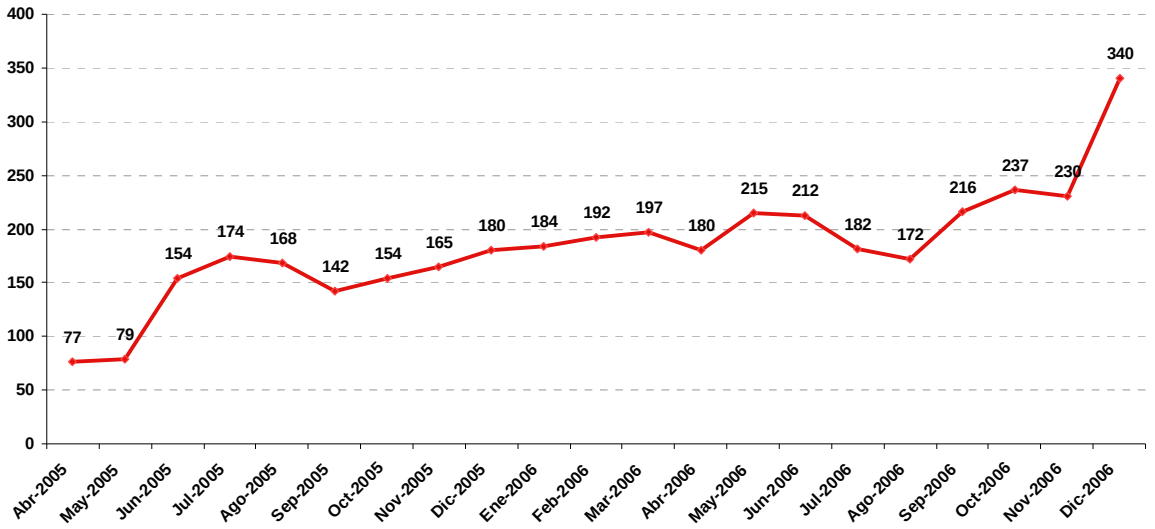
El número de sitios web fraudulentos orientados a realizar fraude tuvo un crecimiento del 100% en 2005. Sin embargo, fue en 2006 cuando el número de webs fraudulentas se multiplicó por 10, lo que se explica por la sofisticación de los ataques y por el uso de otros medios de comunicación, distintos del correo electrónico, para engañar al usuario. Los ataques basados en código malicioso y *phishing* de motor de búsqueda han aumentado en este periodo, tipos de ataque que no necesitan del uso del correo electrónico ni de otras formas de comunicación directa con la víctima.

A este cambio en la forma de realizar los ataques hay que sumarle la incidencia de nuevos tipos de fraude como el *vishing* o el *smishing* *(Ver pág. 444).*

Otra tendencia a señalar es el notable incremento de la **presencia en la Red de *malware* dirigido a fines fraudulentos**. Al analizar el número de aplicaciones de software malicioso del tipo *keyloggers* y el número de websites que las alojan se ratifican los argumentos anteriores (Gráfico 12).

Así, puede observarse como el número de *keyloggers* orientados al *phishing* ha aumentado en un porcentaje superior al 300% entre abril de 2005 y diciembre de 2006.

Gráfico 12: Número de capturadores de pulsaciones de teclado (*keyloggers*) únicos orientados al *phishing*

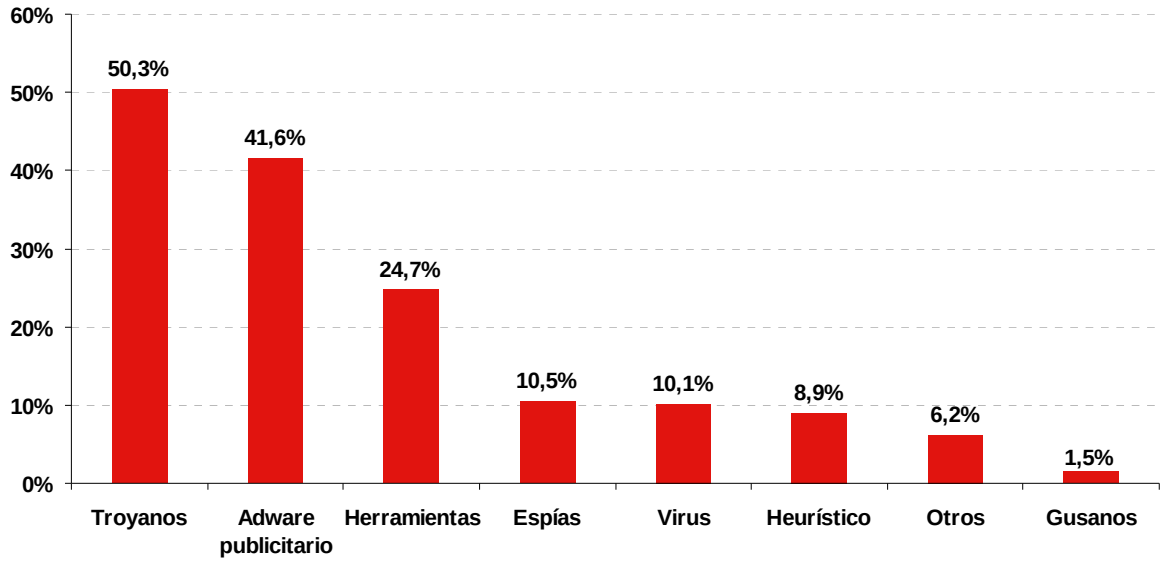


Fuente: APWG

En este sentido, según el estudio de INTECO[31] los capturadores de pulsaciones o *keyloggers* – que son un tipo de malware incluido dentro de la categoría de los troyanos – que más incidencia tiene en la actualidad en los equipos de los hogares españoles, siendo además el código malicioso del que más producción (nuevas variantes únicas) se registra. Así, como se observa en el Gráfico 13 más de la mitad de los hogares españoles tienen, al menos, un troyano en sus equipos.

[31] Primera oleada del "Estudio sobre la Seguridad de la Información y eConfianza en los hogares españoles"

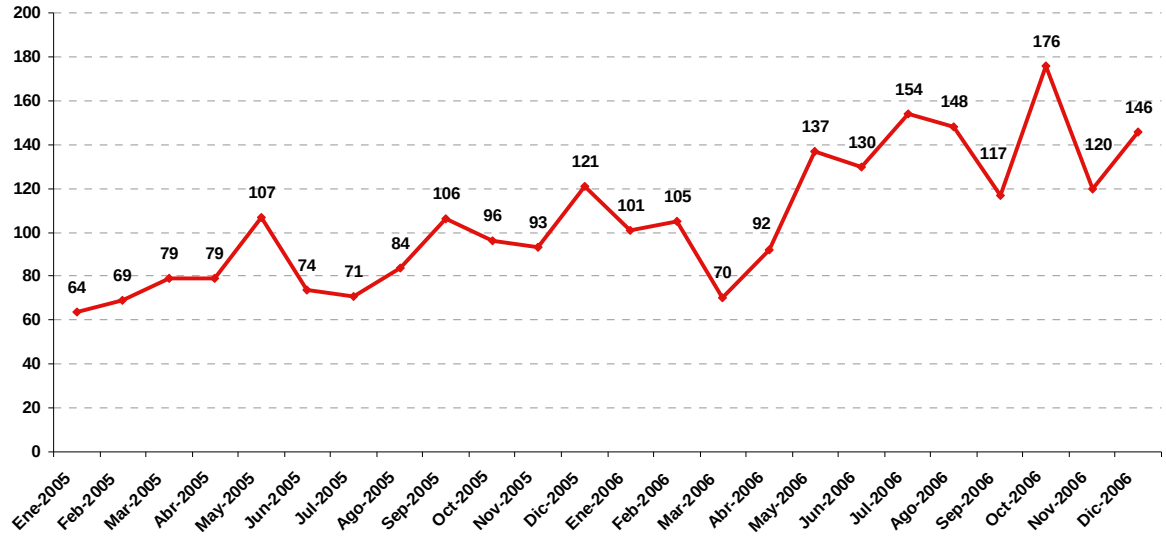
Gráfico 13: Presencia de *malware* por categorías (% sobre el total de ordenadores escaneados)



Fuente: INTECO

Otra medida que también da una muestra de la relevancia del *phishing* es el número de **marcas suplantadas** (Gráfico 14). Esta variable recoge la cantidad de ataques e informa sobre la concentración de éstos.

Gráfico 14: Número de marcas suplantadas por mes

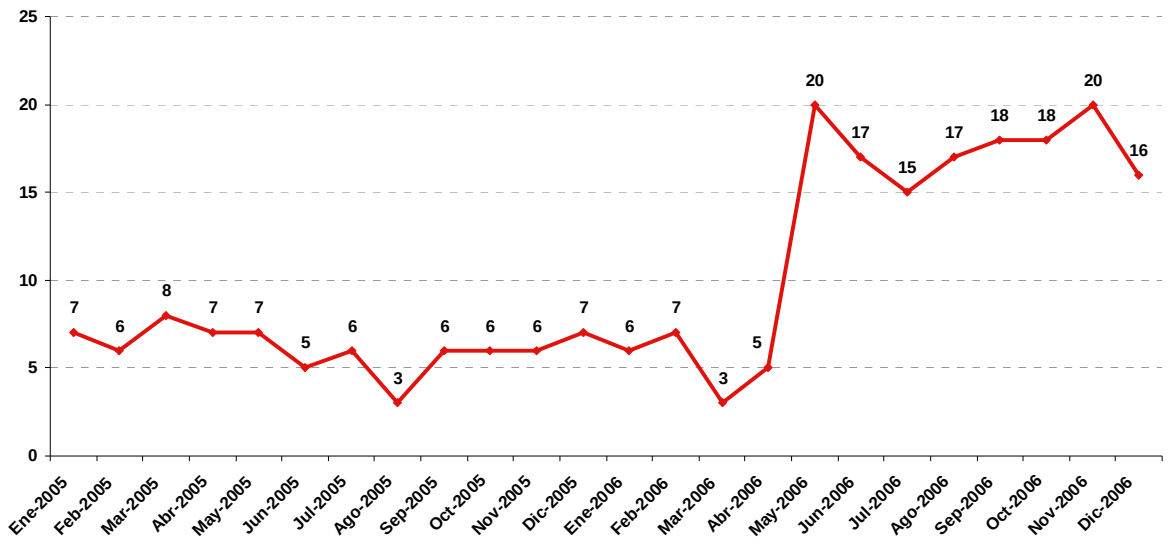


Fuente: APWG

Puede apreciarse como los ataques son cada vez más dispersos, de manera que en lugar de concentrarse en unas pocas entidades financieras como ocurría en enero de 2005, los atacantes han diversificado sus ataques hacia empresas y sectores diferentes para incrementar las posibilidades de defraudar a los consumidores.

También se dispone de una medida de concentración pura: número de marcas suplantadas que acumulan el 80% de los ataques de *phishing*. (Gráfico 15).

Gráfico 15: Número de marcas suplantadas por mes que acumulan el 80% de los ataques



Fuente: APWG

Por lo que se refiere a la **procedencia de los ataques**, Estados Unidos, la República de Corea y China aglutinan más del 50% de los servidores que alojan sitios web de *phishing* como muestra la Tabla 9.

Estados Unidos es el país que registra un mayor porcentaje de servidores de este tipo, si bien se confirma, tras un pequeño incremento en 2005, la descentralización de estos servidores hacia otros países (pasando del 32% para en el año 2004 al 24,7% en el año 2006).

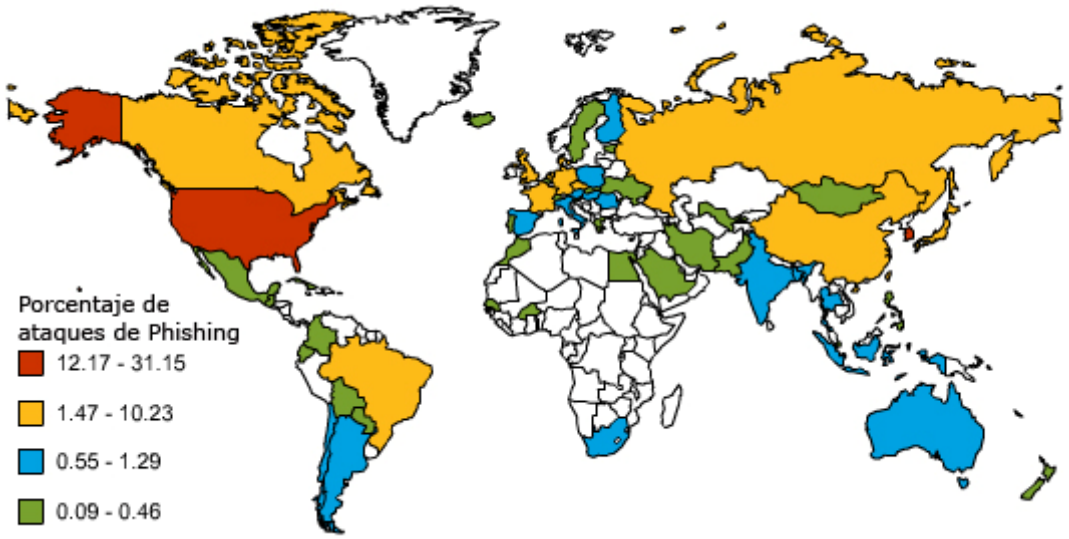
Tabla 9: Clasificación de los diez primeros países en función de los servidores que alojan sitios web dedicados al *phishing*. Años 2004-2006 (%)

Posición	Diciembre 2004		Diciembre 2005		Diciembre 2006	
1º	EEUU	32,0%	EEUU	34,7%	EEUU	24,7%
2º	China	12,0%	Rep. Corea	9,8%	Rep. Corea	15,7%
3º	Rep. Corea	11,0%	China	9,0%	China	14,2%
4º	Japón	2,8%	Alemania	3,8%	Alemania	4,1%
5º	Alemania	2,7%	Reino Unido	3,4%	Canadá	3,1%
6º	Francia	2,7%	Japón	3,3%	Reino Unido	2,7%
7º	Brasil	2,7%	Taiwán	2,2%	Francia	2,2%
8º	Rumania	2,2%	Rumania	2,0%	Japón	1,7%
9º	Canadá	2,1%	Francia	2,0%	Rusia	1,7%
10º	India	2,1%	Canadá	1,9%	Italia	1,7%

Fuente: APWG

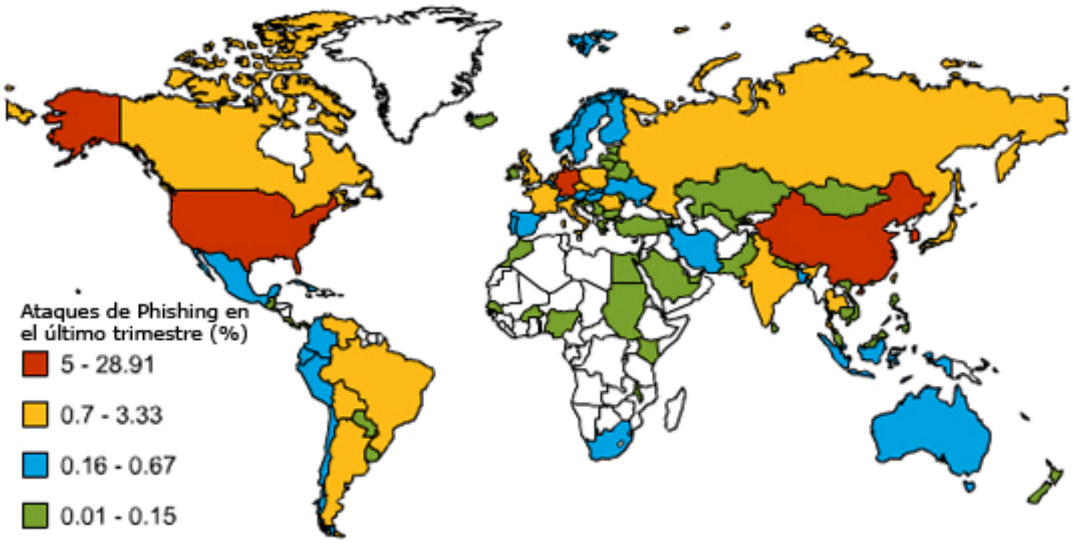
La empresa **Websense Security Labs** (www.websense.com/securitylabs/) calcula y actualiza constantemente su "mapa del *phishing*" (Gráfico 16, Gráfico 17, Gráfico 18), en el que clasifica el lugar desde donde parten los ataques. Se observan a continuación tres momentos diferentes en los que se pueden comprobar las variaciones producidas en el último año: la situación en enero de 2007; en el último trimestre de 2006 (oct.06-ene07) y en el último año (ene06-ene07).

Gráfico 16: Mapa del *phishing* (Websense Security Labs)



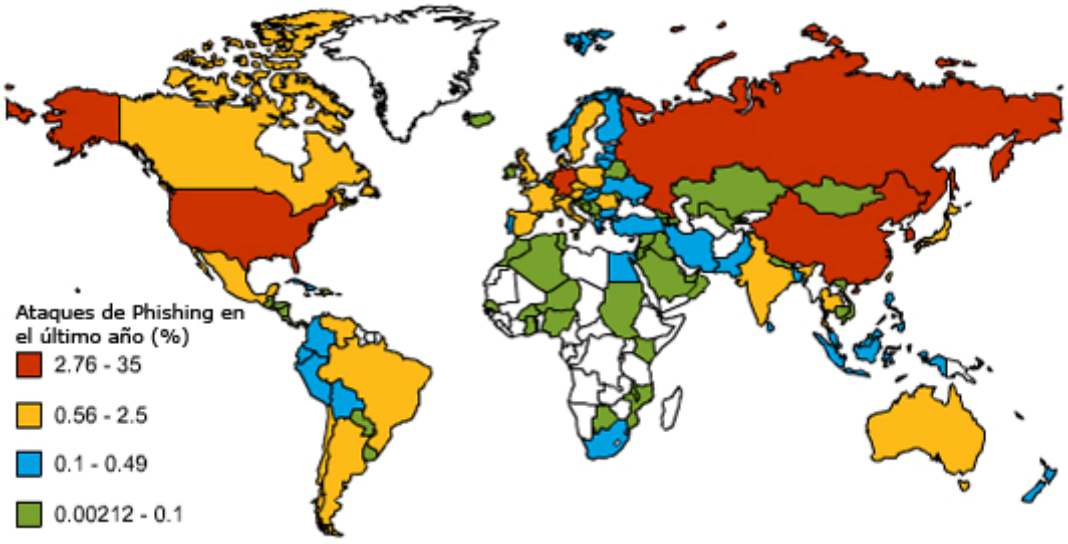
Enero de 2007 *Fuente: Sitio web de Websense Security Labs (2007)*

Gráfico 17: Mapa del *phishing* (Websense Security Labs)



Octubre de 2006-Enero de 2007 *Fuente: Sitio web de Websense Security Labs (2007)*

Gráfico 18: Mapa del *phishing* (Websense Security Labs)



Enero de 2006-Enero de 2007 *Fuente: Sitio web de Websense Security Labs (2007)*

Existe cierta estabilidad en cuanto al orden en el ranking, ocupando los primeros puestos Estados Unidos, China y Corea, mientras que los lugares con menor incidencia del *phishing* son aquellos que muestran un menor nivel de desarrollo económico (algunos países asiáticos, algunas naciones sudamericanas y, sobre todo, el continente africano).

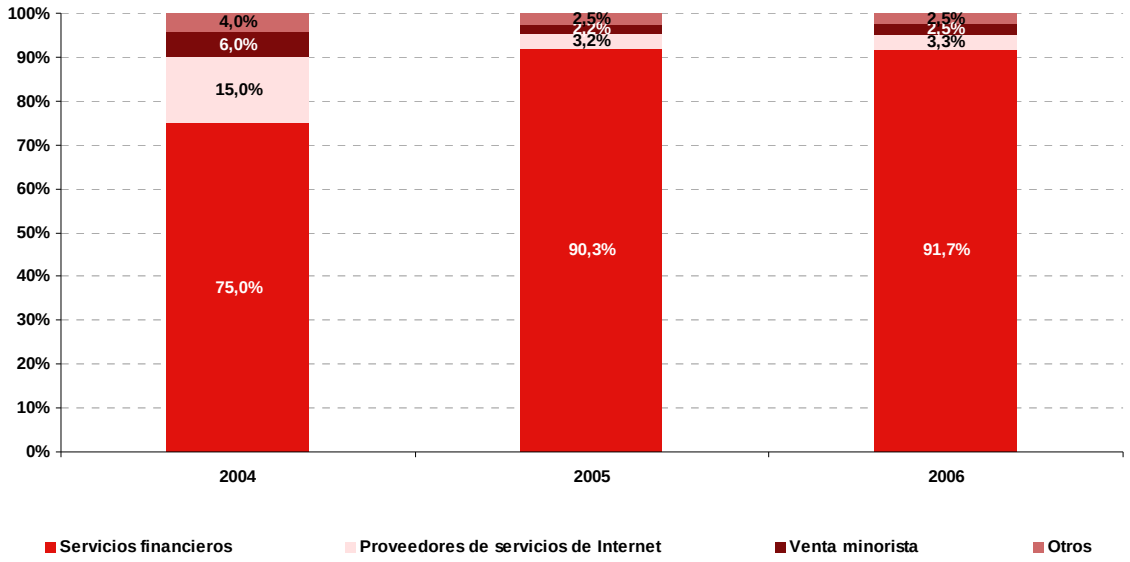
Los grandes países alojadores de webs desde las que se realiza *phishing* son las grandes naciones asiáticas (China, Japón, Corea del Sur), Norteamérica en su conjunto (aunque

parece existir una tendencia decreciente en México) y gran parte de los países de la Unión Europea.

Resulta interesante estudiar cuáles son los **sectores de actividad** en los que los *phishers* centran sus estafas.

La lógica indica, y los datos confirman, que el sector financiero soporta más del 90% de las suplantaciones en los últimos dos años, siendo el sector en el que los *phishers* centran sus ataques (Gráfico 19).

Gráfico 19: Distribución por sectores del *phishing* (%)



Noviembre de 2004-2005-2006 *Fuente: APWG*

En cuanto a los **periodos de tiempo más activos, desde un punto de vista amplio no puede hablarse de estacionalidad en** cuanto al número de ataques de *phishing* durante una determinada época del año.[32]

Como muestra el Gráfico 10, a nivel mundial en el año 2005 se observa un ligero repunte durante los meses estivales en el número de ataques de *phishing,* pero dicha tendencia no aparece en 2006; todo lo contrario se observan marcados aumentos y descensos durante dichos meses. En el caso de España, el Gráfico 26 muestra cómo durante 2005 se

[32] Este punto de vista es compartido por otras fuentes. Así, por ejemplo la empresa de seguridad S21Sec en Agosto de 2007 informaba de la situación de ataques de *phishing* detectados durante la primera mitad de ese año, y al respecto de dicha información concluía que aunque la mayor parte de los ataques de *phishing* se sufrieron en los meses de mayo y junio, s21sec negaba que se pudiese identificar una temporada concreta del año como la de mayor actividad en estos ataques.

http://www.elpais.com/articulo/internet/bancos/sufren/490/variantes/phishing/primera/mitad/2007/elpeputec/20070802elpepunet_10/Tes

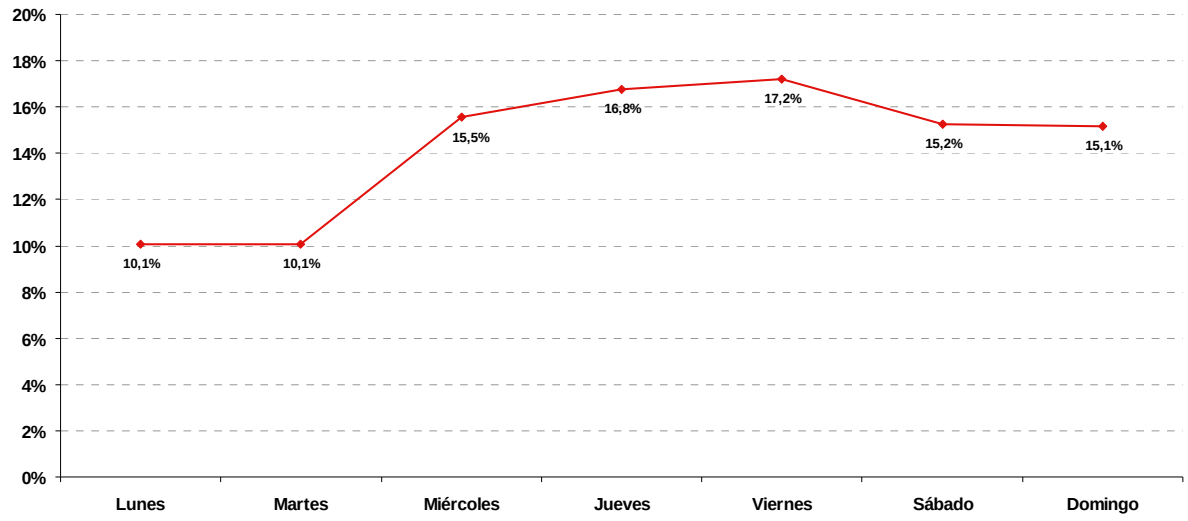
incrementa el número de ataques de *phishing* en el periodo veraniego mientras que en 2006 durante esa misma época se estanca e incluso disminuye el número de ataques.

La ausencia de una tendencia clara tanto a nivel nacional como internacional puede estar motivada por la escasez, dispersión y parcialidad de datos de que se dispone, lo que impide inferir conclusiones al respecto.

De otro lado, si se observan los datos recogidos en el Gráfico 20 respecto al porcentaje de mensajes enviados según el día de la semana, se puede advertir un incremento relevante de los ataques en los tres últimos días laborables. Así, **el viernes es el día que más mensajes de *phishing* se envían**, concentrando el 17,2% de los enviados durante toda la semana.

Los *phishers* tratan de conseguir que los destinatarios respondan justo antes del fin de semana con el objetivo de aumentar el tiempo disponible para la estafa.

Gráfico 20: Porcentaje de mensajes únicos de *phishing* por día de la semana



Fuente: Symantec (2006)

Respecto a las técnicas empleadas en la **suplantación de sitios web**, el APWG ofrece sólo datos acerca de dos técnicas:

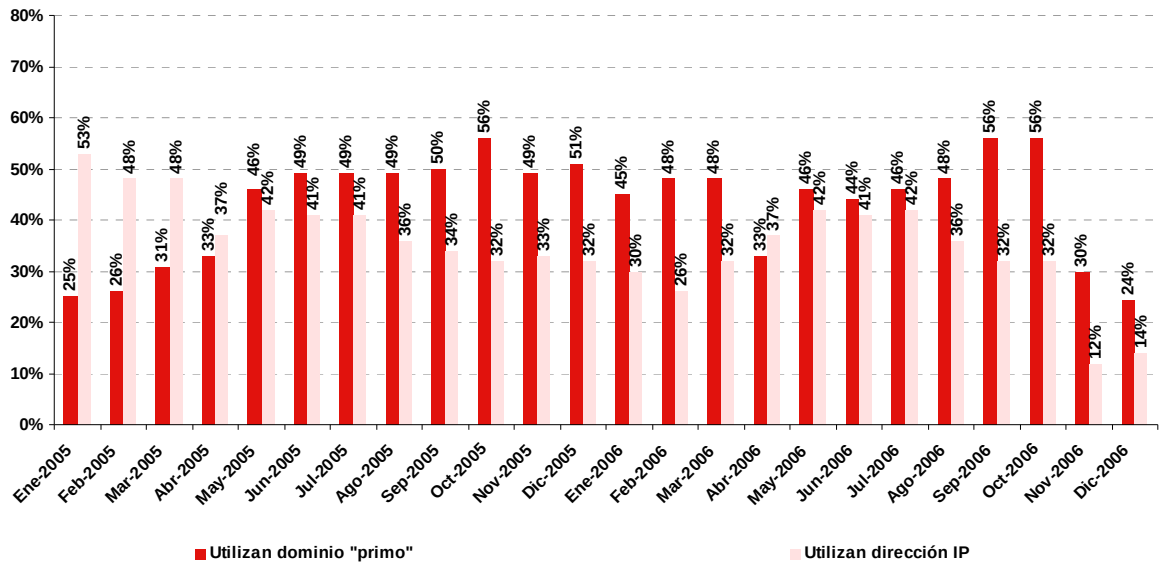
- Técnica de suplantación de páginas web mediante la utilización de dominios "primos". Esta técnica suplanta dominios legítimos mediante la utilización de dominios que recurren a nombres o grafías similares al dominio legítimo, con el fin de confundir al usuario (ej. "www.inleco".es en lugar de "www.inteco.es").

- Técnica de suplantación de páginas web mediante el uso de direcciones IP, en lugar de nombres de dominio. Para comprender mejor esta técnica de suplantación conveniente señalar que el acto cotidiano de visualizar una página web y que se asume como un acto sencillo, encierra determinados procesos.

  Internet utiliza las llamadas direcciones IP (Internet Protocol) que consisten en una serie numérica única. De este modo, al igual que mediante un número, nombre y código postal se localiza un domicilio concreto en una ciudad, la dirección IP se relaciona con una determinada página web. Pero esta cadena numérica no resulta fácil de memorizar, por lo que se utilizan los nombres de dominio mucho más sencillos de recordar. Las DNS (Domain Name Server) traducen estos nombres al lenguaje numérico que necesita Internet para funcionar.

  En el Gráfico 21 se observa la caída proporcional del uso de la dirección IP y el ascenso del uso de dominios "primos".

Gráfico 21: Principales técnicas de suplantación de sitios web (%)



Fuente: APWG

Esta caída se debe al hecho de que en muchas ocasiones el destinatario de la estafa desconoce con exactitud a qué se debe que la dirección que aparece en la barra del navegador sea un conjunto de números, por lo que la desconfianza lleva a que se reduzca la tasa de éxito de este ardid. Por el contrario, la técnica de suplantación de sitios web mediante el uso de dominios "primos" parece ganar terreno. En todo caso, se detecta cierta caída en el uso de ambas técnicas, sobre todo en los últimos meses de 2006. Este hecho encuentra su explicación en dos factores:

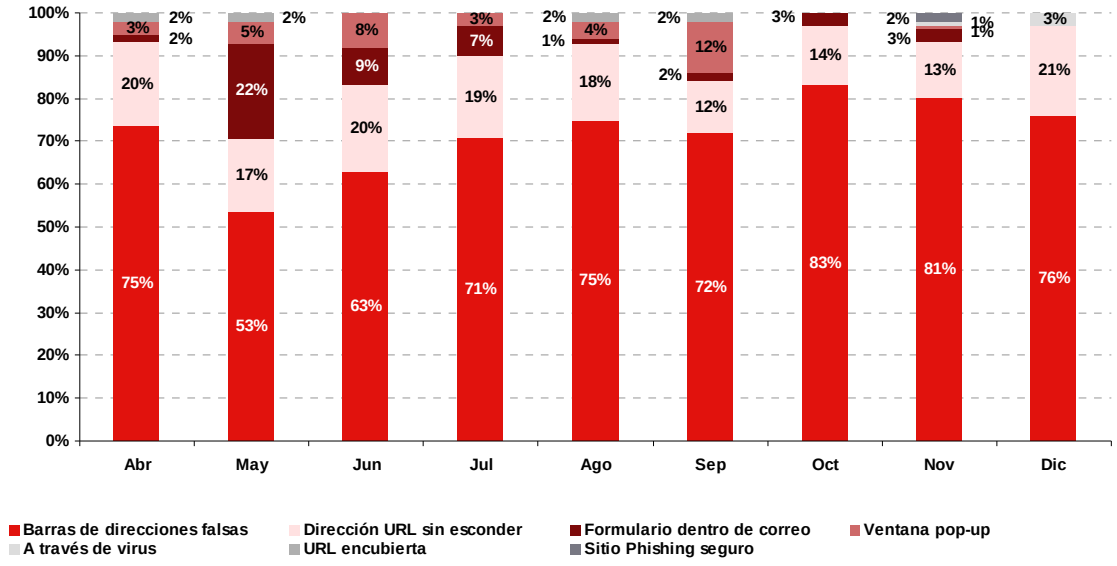
- De un lado, en el mayor conocimiento del usuario de la existencia de este tipo de delitos.

- De otro lado, en el empleo de otras técnicas como las barras de direcciones falsas o la utilización de virus (véase Gráfico 22)

Alternativamente, como se observa en el Gráfico 22, las estadísticas de **Trend Micro** (www.trendmicro.com/vinfo/) analizan un mayor número de técnicas de suplantación, aunque siempre hay que considerar que la muestra la componen únicamente sus clientes.

La caída en la utilización de ventanas emergentes se debe a la incorporación de herramientas para el bloqueo de estas ventanas en prácticamente todos los navegadores. El empleo de esta técnica está muy limitado. Por lo demás, se debe destacar la poca incidencia del resto de técnicas, cuyos valores rara vez superan el 5% y el desuso de los formularios en el correo electrónico gracias a los esfuerzos realizados en la educación de usuarios.

Gráfico 22: Distribución de las técnicas de suplantación de sitios web (%)

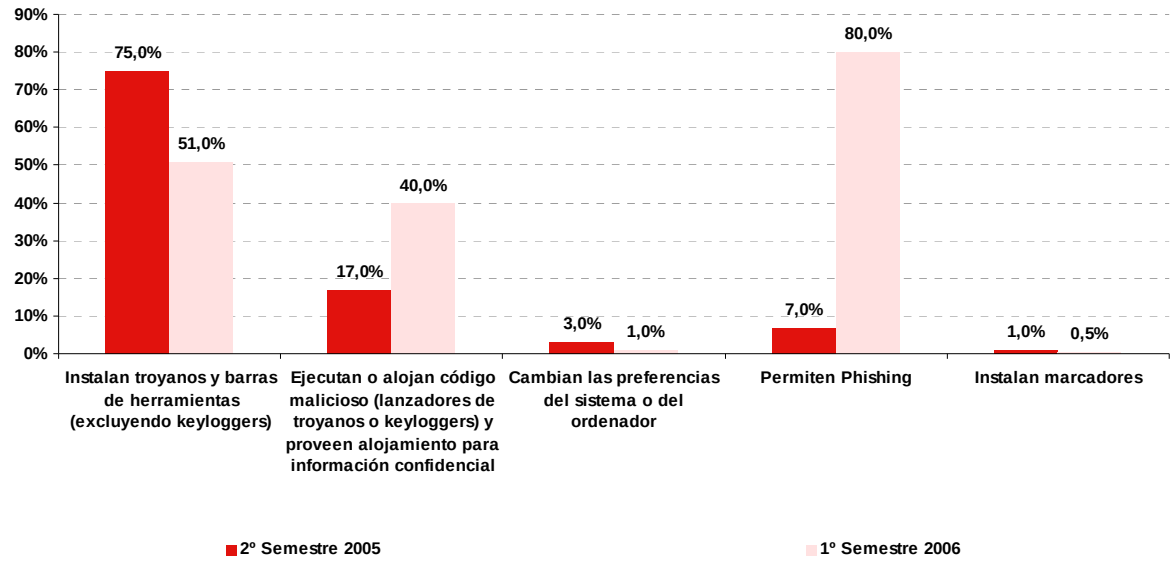


Fuente: Trend Micro (2006)

En cuanto a la **utilización de código malicioso o *malware*** para la realización de *phishing*, el Informe de Websense Security Labs muestra el porcentaje de sitios web con códigos maliciosos de distintos tipos, todos ellos orientados a facilitar este delito.

En este sentido, hay que destacar como muestra el Gráfico 23 el uso de troyanos web y el crecimiento en el primer semestre de 2006 de la incidencia de los *keyloggers*, quizá las variedades más sencillas desde el punto de vista tecnológico y para las que existen los kits de desarrollo a los que se ha hecho referencia a lo largo de este estudio.

Gráfico 23: Porcentaje de códigos maliciosos alojados en sitios web (%)



Fuente: Websense Security Labs (2006)

Respecto a los troyanos y *keyloggers*, el Anti-Phishing Working Group ofrece información interesante sobre dónde se encuentran los servidores que alojan este tipo de aplicaciones.

Destaca, como en casos anteriores, el primer puesto constante de Estados Unidos (42,5% de los servidores en diciembre de 2006), pero también llama la atención el crecimiento de la parte correspondiente a los países asiáticos (Tabla 10).

Tabla 10: Clasificación de los diez primeros países en función del alojamiento de troyanos (incluyendo *keyloggers*) orientados al *phishing*. Años 2005-2006 (%)

Posición	Diciembre 2005		Diciembre 2006	
1º	EEUU	25,6%	EEUU	42,5%
2º	España	14,3%	China	7,7%
3º	Brasil	12,0%	Rusia	4,1%
4º	China	6,0%	Rep. Corea	3,4%
5º	Rusia	4,0%	Brasil	3,1%
6º	Canadá	3,0%	Alemania	2,5%
7º	Argentina	3,0%	España	2,3%
8º	Reino Unido	2,5%	Argentina	2,1%
9º	Países Bajos	2,0%	Italia	1,6%
10º	Suiza	1,0%	Francia	1,3%

Fuente: APWG

A priori, parece que esta situación está controlándose en España, que pasó de ocupar el segundo puesto en diciembre de 2005 con un 14,3% de los servidores con troyanos, a un

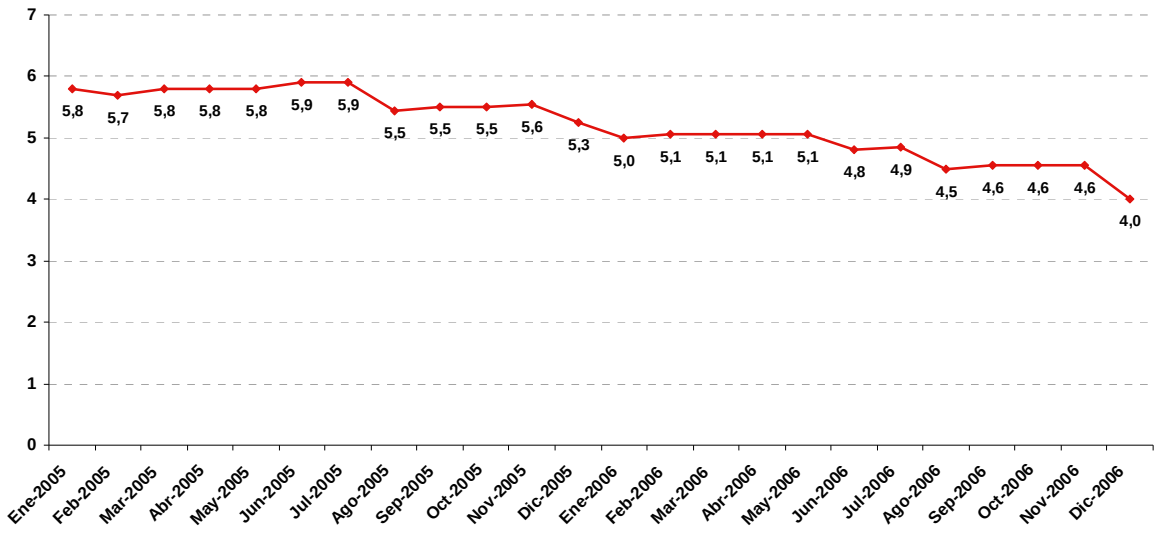
séptimo puesto en diciembre de 2006, donde se midió que sólo el 2,3% de dichos servidores se encontraban en territorio nacional.

Sin duda, esta es una muestra de la extensión de este tipo de códigos maliciosos, en la misma línea observada respecto a las pautas generales de estos delitos.

Finalmente, para cerrar este conjunto de estadísticas de *phishing* a nivel internacional, resulta interesante evaluar el **tiempo medio de apertura de sitios web fraudulentos**.

En este sentido, el APWG recoge el tiempo medio que permanece abierto un sitio fraudulento dedicado a este tipo de actividad. (Gráfico 24). La evolución, aunque relativamente lenta, es positiva. El tiempo medio de apertura de estos sitios se ha reducido de algo más de 6 días a 4 días y medio en los últimos dos años.

Gráfico 24: Tiempo medio que permanece abierto un sitio web fraudulento



Fuente: APWG

Para el caso de España y siguiendo el Informe sobre Fraude Online 2006 que elabora **S21sec**, y en el cual colabora INTECO; el tiempo medio de cierre de los casos de fraude detectados por la compañía se sitúa en 2,56 días, muy por debajo de los datos proporcionados por APWG que sitúa la media de cierre global en 4,8 días. Analizando exclusivamente los casos de *phishing*, la media de tiempo empleado por los servicios antifraude de esta compañía fue de 1,63 días para los casos base (casos que se abrían por primera vez) y de 1,76 para las reaperturas de algunos de los casos ya existentes.

Conclusiones derivadas de las estadísticas del *phishing* a nivel mundial

Tras observar las distintas estadísticas internacionales que se han presentado, se pueden extraer una serie de conclusiones:

- Crecimiento considerable de los fraudes de *phishing*. Como se observaba en el Gráfico 10 desde enero de 2005 hasta diciembre de 2006 el número de ataques ha aumentado un 100%. Destaca el incremento sufrido en el número de ataques a partir de abril del 2006. Para España, como se mostrará en el Gráfico 26, la evolución ha sido desigual: gran crecimiento hasta octubre de 2005, descenso a lo largo del año 2006 y repunte al final de ese año.

- Creciente sofisticación de los ataques. El mayor incremento de los sitios web dedicados al *phishing* respecto al envío de correos electrónicos es una clara muestra del empleo de otras variantes dentro de este tipo de estafa. Las estadísticas muestran la creciente incidencia del *phishing* basado en el uso de código malicioso (*malware*) que a diferencia del *phishing* original precisa no sólo del engaño que subyace en cualquier timo o estafa, sino de un conocimiento avanzado por parte del *phisher* en la creación y/o utilización de código malicioso. El fraude online evoluciona hacia la creación de las llamadas amenazas silenciosas. Así los creadores de código malicioso centran su producción en programas que pasen inadvertidos para el usuario: troyanos, *rootkit*, etc.[33].

- El incremento de ataques "enfocados". El incremento en el número de marcas suplantadas y la menor concentración de los ataques son muestra de dos factores: la búsqueda de nuevos mercados por parte de los delincuentes y, sobre todo, la entrada de nuevos estafadores.

- El principal país origen de los ataques de *phishing* es Estados Unidos, con una cierta distancia respecto al resto de países. Sin embargo, la dispersión geográfica cada vez mayor viene a avalar las conclusiones respecto a la entrada de nuevos focos de producción del *phishing*.

- La predominancia del sector financiero como objetivo de estos delincuentes es evidente e incluso se ha agudizado en los últimos años.

- Las estadísticas respecto al cierre de sitios de *phishing* apuntan una mejora en la lucha contra este delito. La lucha, a través de la cooperación internacional entre entes públicos y privados, se intensifica, ayudando a eliminar las posibles barreras que puedan existir, para erradicar estos sitios.

[33] Más del 50% de los equipos de los hogares españoles albergan código malicioso de este tipo, como se recoge en la Primera Oleada del Estudio sobre la Seguridad de la Información y eConfianza de los Hogares Españoles (INTECO 2006)

- Aunque el APWG posee una buena base de datos a nivel internacional, se detecta cierta dispersión en las estadísticas, que va en detrimento de un mejor conocimiento del comportamiento de estos delincuentes. Actuaciones encaminadas a documentar de forma más extensa estos delitos serán fundamentales en la lucha contra ellos.

2.4.1 El *phishing* en España

Principales fuentes de datos

En España debemos destacar la labor realizada por el **Ministerio de Industria, Comercio y Turismo** (www.mityc.es) a través de la entidad pública **Red.es** (www.red.es) y **el Instituto Nacional de Tecnologías de la Comunicación –INTECO-** (www.inteco.es). Estas entidades han colaborado con otras instituciones para la realización de diversos estudios sobre la situación del comercio electrónico en España y el avance de las tecnologías de la información y las comunicaciones.

Respecto a las fuentes de datos españolas, destaca el papel del **Instituto Nacional de Estadística –INE-** (www.ine.es), que realiza dos encuestas, una sobre tecnologías de la información en los hogares y otra sobre el uso de esta tecnología y del comercio electrónico en las empresas, en las cuales se introducen algunas consideraciones sobre seguridad informática.

Finalmente, dos son los informes que de manera más directa tienen como objetivo el estudio de la situación española: el realizado por la **Asociación de Internautas -AI-** (www.internautas.org) (en sus versiones de 2005 y 2006) y el publicado por **S21sec** (www.s21sec.com) **y Verisign** (www.verisign.com), centrándose este último en ataques a entidades financieras.

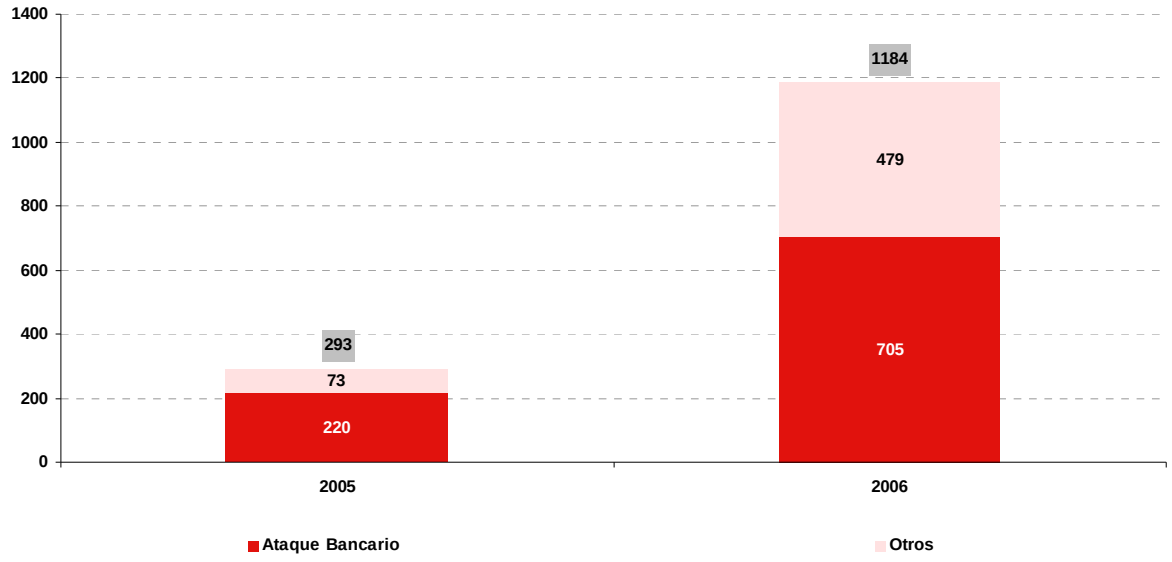
Si bien las fuentes de información públicas sobre este delito no son abundantes y presentan inconsistencias, existen algunos elementos de interés que ofrecen pistas sobre su evolución en España.

Principales variables analizadas

Como se observa en el Gráfico 25 el **crecimiento del *phishing* en España** entre los años 2005 y 2006 fue superior al 300% pasando de 293 ataques en 2005 a 1.184 en 2006.

Especialmente relevante resultó el incremento de ataques no bancarios, que alcanzó cotas superiores al 500%. Este incremento viene motivado en gran medida por el aumento de ataques de *scam* (ofertas de trabajo online de carácter fraudulento) de la que se registraron 344 casos en 2006.

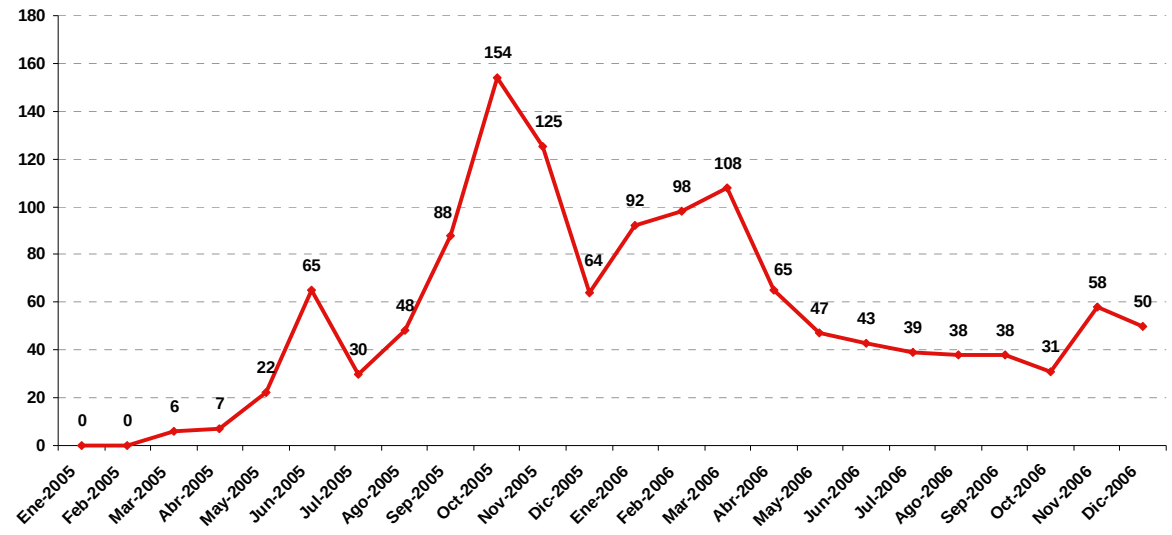
Gráfico 25: Evolución del número de ataques de *phishing* por tipo en España



Fuente: Asociación de Internautas

De modo similar, el informe publicado por **S21sec y Verisign** (2006) y el informe de **S21sec, Indra** (www.indra.es) **e Inteco** (2007) relativos a la evolución del *phishing* en 2005 y 2006 sobre la base de clientes de S21sec, mostraban datos poco alentadores, con una aceleración muy acusada en muy pocos meses. En el Gráfico 26 puede observarse como se produce un notable crecimiento hasta octubre de 2005, momento en el que comienza a descender hasta finales de 2006.

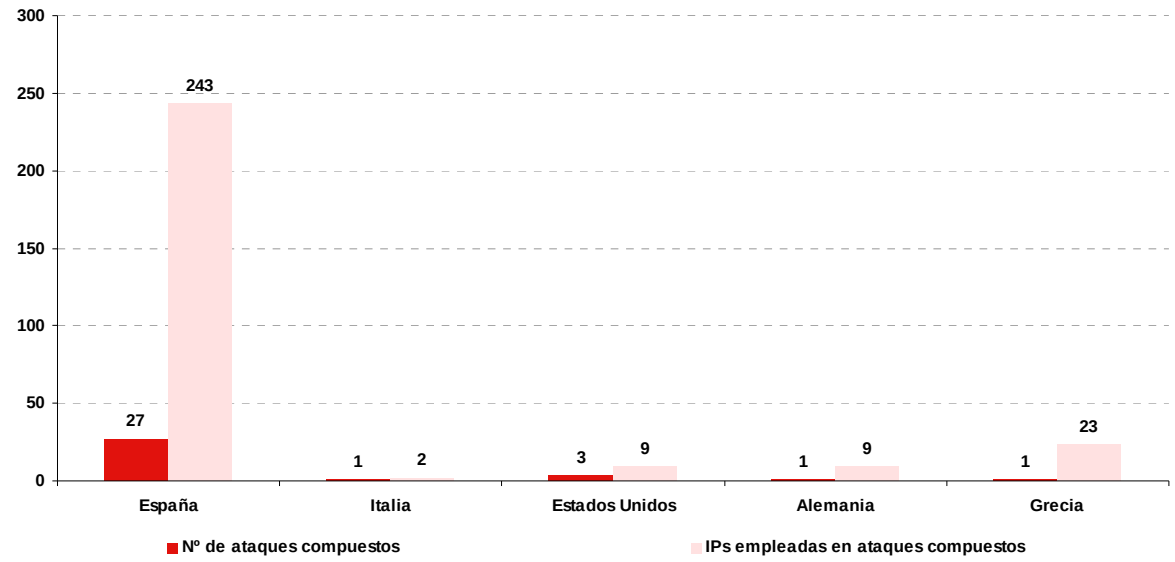
Gráfico 26: Número de ataques de phishing en España



Fuente: S21sec y Verisign

A la reflexión ante dichas cifras ha de sumarse el hecho de que paulatinamente se aprecia una cierta sofisticación en los delincuentes que operan en España, tal y como señalan los datos sobre ataques mixtos[34] desarrollados en nuestro país (Gráfico 27).

Gráfico 27: Número de ataques mixtos e IPs utilizadas



Fuente: S21sec y Verisign (2006)

En relación con el **código malicioso destinado a servir de herramienta para el *phishing***, España se sitúa en niveles intermedios-altos respecto a la ubicación de servidores que alojen estas aplicaciones, con cierta tendencia descendente. Analizando individualmente los datos proporcionados por el APWG en relación con los sitios web que alojan dos tipos concretos de *malware* (*keyloggers* y troyanos web orientados a la realización de *phishing*), se confirma esta tendencia[35]. (Gráfico 28).

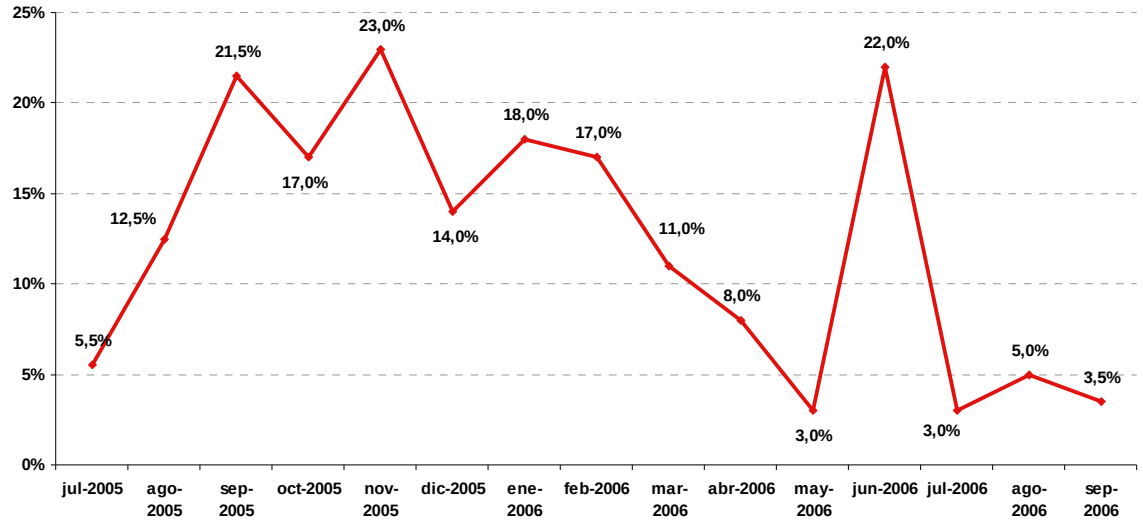
Durante el año 2006 se produce un descenso continuado en el porcentaje de servidores españoles que alojan capturadores de pulsaciones de teclado (*Keyloggers*) y troyanos web para la realización del *phishing* hasta el mes de mayo en el que se inicia una subida creciente hasta junio de 2006, mes en el que se registró un máximo histórico mundial de intentos de fraude bancario a través de Internet, según datos del APWG y que se muestran en el Gráfico 10.

[34] Según el informe de S21sec y Verisign, los ataques mixtos son casos en los que "el atacante, al principio de modo manual, y después de modo automático, hace que la dirección IP de destino sea 'cambiante de modo dinámico'. El ataque se realiza desde un dominio, recientemente registrado, y que no tiene nada que ver con el nombre de la entidad atacada (por ejemplo, www.123fgh.com). Este nombre de dominio está dirigido a una dirección IP que va cambiando al cabo de unas horas, de modo que el cierre de un sitio fraudulento en un ISP (dirección IP) se ve inmediatamente seguido de la apertura de otros sitios fraudulentos, en diferentes países, haciendo mucho más complicada la lucha contra este tipo de fraude".

[35] De hecho, el APWG elabora un "top 10" de los países respecto a esta variable. Curiosamente, en los datos publicados para octubre y noviembre de 2006, por primera vez en más de un año, España desaparece de esos puestos de cabeza, no habiendo datos disponibles sobre cuál es el porcentaje de estos sitios que se sitúan en dicho país.

No obstante, como se apuntaba en la introducción del capítulo 2.4 "El *phishing* en cifras", a la hora de abordar un análisis del fenómeno del *phishing* conviene tener presente en todo momento la **escasez, dispersión y parcialidad de los datos estadísticos** disponibles actualmente. Por ello, sería muy deseable, que a través de la coordinación de diferentes entidades y organizaciones, se facilitase información veraz sobre la situación real del *phishing*, en particular, y del fraude a través de Internet en general, con la finalidad de construir indicadores que puedan orientar en que dirección se debe avanzar, y las medidas de prevención que se deben adoptar.

Gráfico 28: Evolución del porcentaje de servidores españoles que alojan capturadores de pulsaciones de teclado (*keyloggers*) y troyanos web para la realización de *phishing*



Fuente: APWG

En cualquier caso, hay que tener en cuenta que no todos los ataques que tienen como objetivo España tienen su **origen** dentro de sus fronteras. Siguiendo con las estadísticas del informe de S21sec y Verisign, se comprueba cómo la mayor parte de esos ataques procedían del extranjero, tal y como muestra el Gráfico 29 (sólo 10 de los 609 casos analizados en el informe tenían su origen en España, menos del 2%). Por tanto, aunque se puede afirmar que España no parece ser la mejor ubicación como base de operaciones para los ciberdelincuentes, sí parece que se constituye un objetivo de sus ataques.

Esta idea viene corroborada por los últimos datos publicados. Un reciente informe del Centro de Mando Antifraude de la empresa de seguridad norteamericana **RSA**[36] (www.rsa.com) afirmaba que el mes de julio se ha convertido en el tercer mes con mayor

[36] http://www.laflecha.net/canales/seguridad/noticias/el-phishing-crece-un-4-en-julio-y-en-espana-las-entidades-acumulan-46-ataques-en-un-mes?from=rss

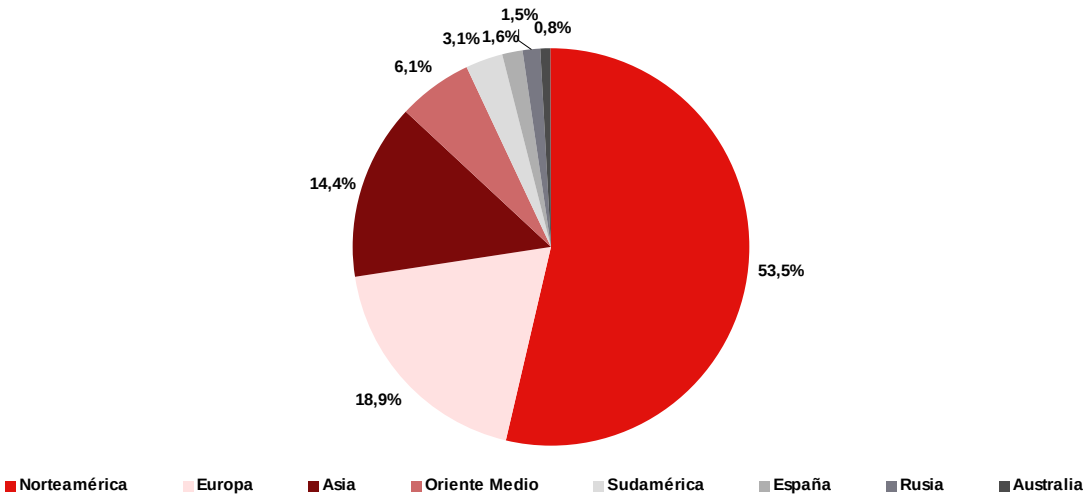
número de ataques hasta el momento, confirmándose que los ataques de phishing siguen en línea ascendente. Así, los ataques de *phishing* han aumentado un 4% sólo en el mes de julio, hasta afectar a un total de 191 entidades en todo el mundo, 15 en el mes precedente.

Según esta fuente, **España se sitúa en el tercer puesto de países más atacados, con un 6% de los intentos**, mismo porcentaje que Canadá. En los datos de RSA se observa que sólo **en julio de 2007, España ha sufrido un total de 46 ataques, en su mayoría provenientes de Estados Unidos, dirigidos en su totalidad a sólo 10 entidades**.

Estados Unidos sigue en primera posición, con el 63% de ataques, frente al 70% del pasado mes. Por el contrario Reino Unido, que ocupa el segundo lugar, ha contabilizado el 12% de los ataques, frente al 9% del mes anterior.

Además, Estados Unidos sigue siendo el país que genera más ataques de este tipo y continúa incrementando su número en julio, con el 66%, frente al 59% del mes anterior. Hong Kong sigue en segundo lugar con el 10%, seguido de Francia, Reino Unido y Canadá.

Gráfico 29: Áreas de procedencia de los ataques de fraude online en España (%).

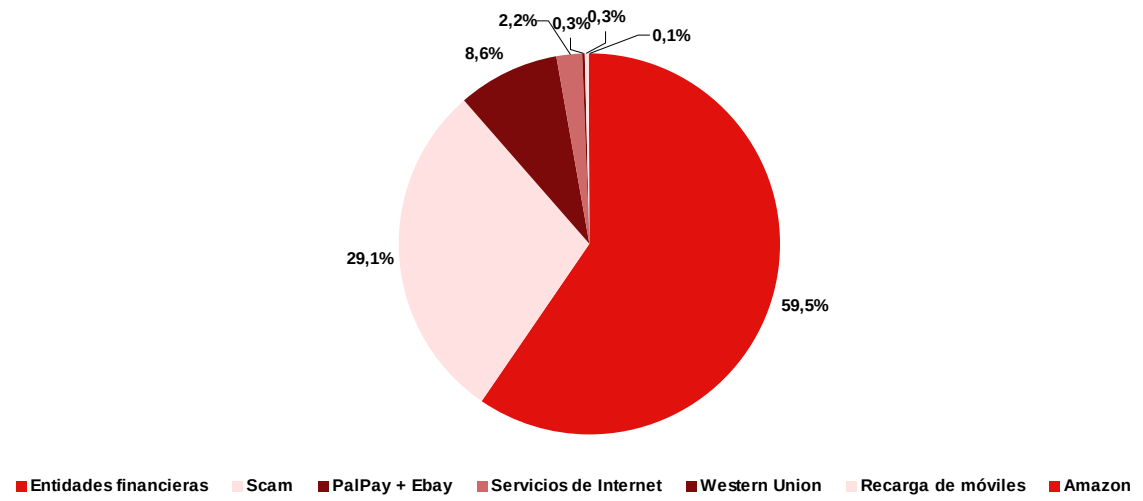


Fuente: S21sec y Verisign (2006)

Atendiendo a las **marcas suplantadas**, las estadísticas sólo se refieren a los casos de entidades financieras, pero, al igual que a nivel internacional, estos casos constituyen la mayoría de los fraudes de *phishing* que se llevan a cabo en España.

Según las estadísticas publicadas en 2006 por la Asociación de Internautas (Gráfico 30) alrededor del 60% de los casos registrados tenían como entidad suplantada un banco, una caja de ahorros o algún otro tipo de institución financiera.

Gráfico 30: Distribución del porcentaje de casos de *phishing* en España



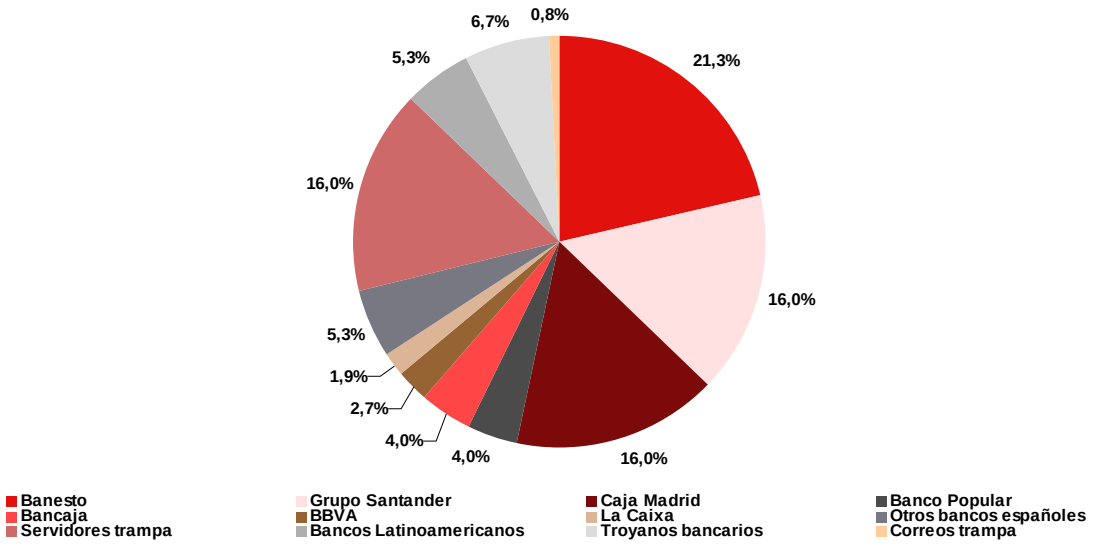
Fuente: Asociación de Internautas

También son muy numerosos (cerca del 30%) los casos de *scam* considerados por la Asociación de Internautas. Este tipo de práctica no siempre implica la suplantación de alguna compañía, aunque los delincuentes se hicieron pasar en varias ocasiones por ONGs con fines humanitarios.

Ebay (www.ebay.es) y PayPal (www.paypal.com) destacan, como también sucede a nivel internacional, entre el resto de casos analizados. Fuera de estas tipologías, los ataques han sido marginales.

También cabe señalar, como se recoge en el Gráfico 31, la localización de 127 servidores trampa y de 47 troyanos, todos ellos con la única finalidad de obtener datos bancarios para realizar este tipo de fraudes. Este hecho confirma el "interés" que los delincuentes tienen en nuestro mercado y la mayor incidencia de ataques más sofisticados.

Gráfico 31: Distribución de los casos de *phishing* en España



Fuente: Asociación de Internautas (2006)

Conclusiones derivadas de las estadísticas del *phishing* para España

Se expone a continuación, en la misma forma que desde el punto de vista internacional, una serie de conclusiones derivadas de la exposición estadística nacional presentada:

- La tendencia de este tipo de estafas en el mercado español, al igual que en el resto del mundo, ha sido creciente. Aunque su aparición ha sido más tardía que en otros países, su irrupción ha sido fuerte, con un crecimiento cercano al 300% en el último año.

- Tiene especial relevancia el *phishing* con un mayor contenido tecnológico. Han proliferado significativamente los troyanos bancarios y los ataques mixtos[37].

- La mayor parte de los ataques que tienen sus víctimas en España vienen del exterior. Servidores norteamericanos son el origen de más del 50% de ellos.

- Al igual que en el resto del mundo, el sector más afectado es el financiero.

- A pesar de los esfuerzos realizados por determinadas instituciones y empresas, se detecta cierta carencia de datos a nivel nacional. En la tarea de erradicar este tipo

[37] Según el informe de S21sec y Verisign, los ataques mixtos son casos en los que "el atacante, al principio de modo manual, y después de modo automático, hace que la dirección IP de destino sea 'cambiante de modo dinámico'. Para más información ver nota al pie número 34.

de fraudes es muy útil contar con mediciones estadísticas que ayuden a comprender mejor el problema y orienten las posibles soluciones.

2.4.2 El impacto económico y social del *phishing*

Con objeto de completar el análisis del fenómeno del *phishing*, es necesario hacer referencia al impacto económico y social que este puede llegar a producir. De hecho, sin dichos impactos, como ocurre en cierta medida con algunos tipos de correos electrónicos no deseados, el *phishing* no sería un problema grave.

En este sentido, se va a plantear, mediante una serie de descripciones, cuáles son las pérdidas generadas por el *phishing* tanto para el usuario particular directamente afectado (pérdida de información sensible, pérdida económica) como a las empresas (pérdida efectiva de clientes, pérdida de confianza por parte clientes, pérdida de imagen corporativa o de marca) y, finalmente, a la sociedad en su conjunto, ya que se frena las posibilidades de la floreciente economía digital, en particular, y de la Sociedad de la Información, en general.

Impacto económico

Existen datos de pérdidas económicas del fraude por Internet, tanto para empresas, como para usuarios particulares. Hay que tener presente que estos datos no son muy abundantes dada la reciente aparición del fraude online, y la complicada estimación de los valores económicos implicados en el tema.

Los resultados estadísticos del Estudio obtienen como dato particular un **daño medio cuantificado de 593€, por cada fraude exitoso**[38]. No obstante, la mayoría de los fraudes online con perjuicio económico no representan cantidades económicas elevadas. Así, **en España,** algo más de **2 de cada 3 fraudes**[39] **online** conllevan un perjuicio económico **inferior a los 400€**.

Este es un elemento diferenciador de este tipo de fraude, dado que el objetivo final son cantidades inferiores de dinero pero con ataques exitosos a un mayor número de usuarios. En el ordenamiento jurídico español, la cuantía de 400€ es el límite para considerar el fraude, con perjuicio económico, por Internet como falta. Si la cifra del fraude es inferior a los 400€ se considera falta, en caso contrario se considerará el fraude como delito.

[38] El número de individuos muestrales que reconocen haber sufrido un perjuicio económico con origen en un fraude online es pequeño: de los 3.076 individuos encuestados, únicamente 65 declaran haber sufrido un perjuicio económico. El cálculo del daño medio se hace a partir de las declaraciones de los encuestados. De este modo, teniendo en cuenta el escaso porcentaje de afectación y que el perjuicio se calcula en base al daño declarado, el valor estimado puede sufrir una variabilidad significativa entre muestras sucesivas.

[39] Al igual que sucede con el valor medio, el porcentaje de fraudes que constituyen falta puede sufrir una variabilidad significativa entre muestras sucesivas.

En consecuencia, este criterio económico que delimita el delito de la falta, hace que en muchos casos que los ciberdelincuentes orienten su objetivo hacia estafas de pequeña cuantía, para no solo no ser detectado por los usuarios[40] sino tampoco poder ser acusado de un delito.

A nivel internacional, un reciente Informe sobre delitos en Internet juzgados en Estados Unidos entre 1999 y 2006[41], da muestra de la gravedad de las prácticas de suplantación de identidad. Los ataques de este tipo causaron unas pérdidas medias a las empresas mucho más elevadas que las procedentes de virus y códigos maliciosos en general. De hecho, los ataques mediante acceso por suplantación tuvieron un coste medio de 1,5 millones de dólares por caso, mientras que los costes medios de un ataque a través de código malicioso (por lo general, virus) fue de 2.400 dólares por caso. De este modo, aunque a nivel de conjunto los virus provocan más daño, porque afectan a más empresas, a nivel individual los daños por suplantación son aún mayores[42].

Los datos de la **Federal Trade Commision**[43] sobre robo de identidad y su relevancia son reveladores de una tendencia creciente del problema del *phishing*:

- El problema ha crecido notablemente en los últimos años, pasando de incrementos del 10% a aumentos del 80%.
- Las estadísticas del Departamento de Justicia de los Estados Unidos[44] sitúan al robo de identidad como el delito más importante del país, por delante del tráfico de estupefacientes.
- El coste estimado de perseguir cada delito de estafa financiera asciende a 20.000 dólares. Para una empresa, el robo de la información contenida en un ordenador puede suponer una pérdida de 90.000 dólares.
- El coste para una empresa de cada registro de información sustraído fue de 182 dólares en 2006, frente a los 138 del año anterior.

[40] La relativa escasa cuantía de los fraudes - el Gráfico 37 muestra como más del 75% de los fraudes son de una cuantía pequeña (menos de 500€) y un 24,8% no alcanzan los 50€ – contribuye a que en muchas ocasiones los fraudes no sean detectados por el usuario al camuflarse entre los apuntes bancarios corrientes, y por tanto no sean conocidos ni denunciados. Del mismo modo, ese perjuicio "moderado", hace que en numerosos casos las víctimas, aun conociendo la estafa, minimicen el ilícito y decidan no poner el hecho en conocimiento a las autoridades.

[41] Elaborado por **Trusted Strategies para Phoenix Technologies** (www.trustedstrategies.com)

[42] El informe citado refiere un caso en el que el daño ocasionado por suplantación fue cercano a los 10 millones de dólares.

[43] www.ftc.gov

[44] www.usdoj.gov/criminal/fraud/*Phishing*.pdf

- El coste total (sumando directos e indirectos) para las empresas y consumidores del robo de identidad en 2005 pudo ascender a 56.600 millones de dólares en 2005.

Impacto social

Más allá de las cuantiosas pérdidas monetarias, uno de los efectos negativos del *phishing* es el freno que supone al desarrollo de una economía basada, cada vez más, en transacciones electrónicas, por la desconfianza que se genera en los sistemas de seguridad.

En 2005, un estudio norteamericano[45] – relativo a los aspectos que los usuarios de Internet consideraban más importantes tras su experiencia en este medio – cuya finalidad era analizar la evolución respecto a un informe previo desarrollado en 2002, señalaba que el factor más importante para el usuario a la hora de decidirse a entrar en una web era la capacidad para conservar la privacidad de la información transmitida. Así, este aspecto de la privacidad, aparece como una nueva preocupación relevante de los usuarios de Internet, que prácticamente no era valorada en el anterior estudio.

Estos datos son indicativos de la existencia de algún grado de preocupación sobre la posibilidad de robo de su información de carácter personal a través de la Red. Entre los motivos para no haber realizado nunca compras en Internet, un 68,2% de los encuestados señalan la preocupación por la seguridad al dar detalles de sus tarjetas de crédito[46].

Informes internacionales[47] aportan datos muy reveladores sobre el sector financiero, el más sensible en relación al riesgo.

- El 72% de los usuarios de Internet que no utilizan actualmente la banca online lo haría si hubiera mejoras en la seguridad cuando, en realidad, los problemas no son tan graves.

- El 90% de los actuales usuarios de servicios de banca electrónica accedería a nuevos servicios si su identidad estuviera mejor protegida.

- La seguridad influye en un 65% de las personas a la hora de elegir con qué banco online operar.

[45] Consumer Reports webwatch (2005) www.consumerwebwatch.org

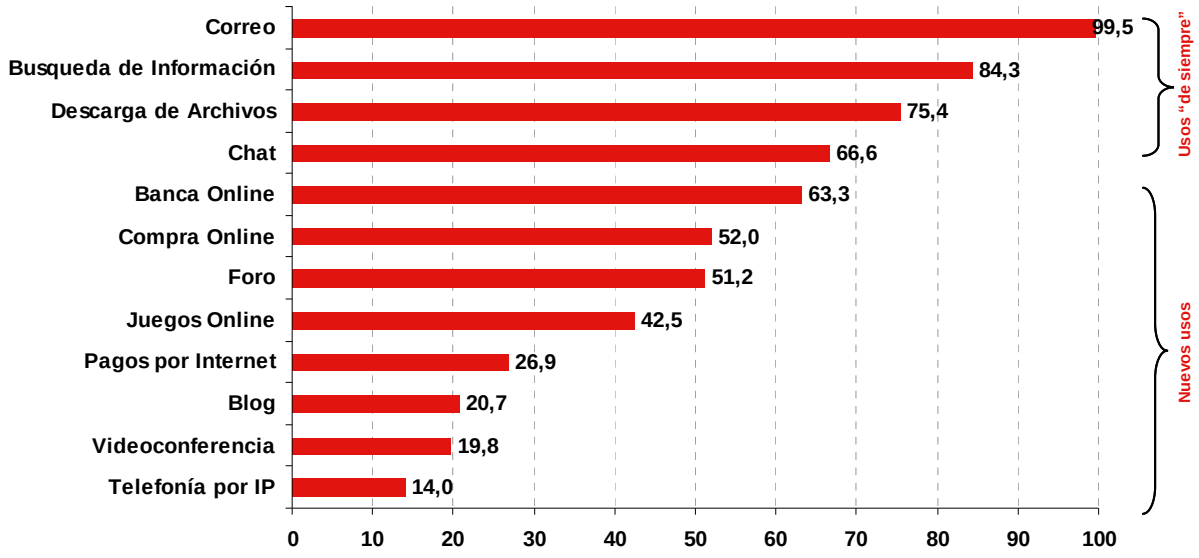
[46] INE: "*Encuesta sobre Equipamiento y Uso de Tecnologías de la Información y Comunicación en los hogares 2º semestre 2006*"

[47] Estudio elaborado por Entrust (2005)

Un 22% de los actuales usuarios estarían dispuestos a cambiar de entidad financiera para garantizarse mejoras en la protección de sus datos. En este sentido – según los datos obtenidos por INTECO en su encuesta a más de 3.000 usuarios de Internet – esta disposición al cambio se convierte en cambio efectivo de entidad bancaria tras haber sufrido un intento de fraude si bien con distinta incidencia según la existencia o no de perjuicio económico. En un 4% de los usuarios que han sufrido un intento de fraude con perjuicio económico este hecho ha motivado un cambio de prestador del servicio banca online, mientras que cuando no existe prejuicio económico el porcentaje se reduce hasta el 1% (Gráfico 43).

Por lo que se refiere a España, se presenta en el Gráfico 32 el porcentaje de utilización de los distintos servicios que ofrece Internet ordenados de forma descendente. Se observa que la utilización de servicios como el correo electrónico, la búsqueda de información y las descargas de archivos tienen una implantación generalizada: en todos los casos, mayor del 75% y casi el 100% en el caso del correo electrónico. Otros servicios que ofrece Internet como la banca electrónica y las compras online muestran también una considerable penetración (más del 50%).

Gráfico 32: Servicios de Internet utilizados (%)

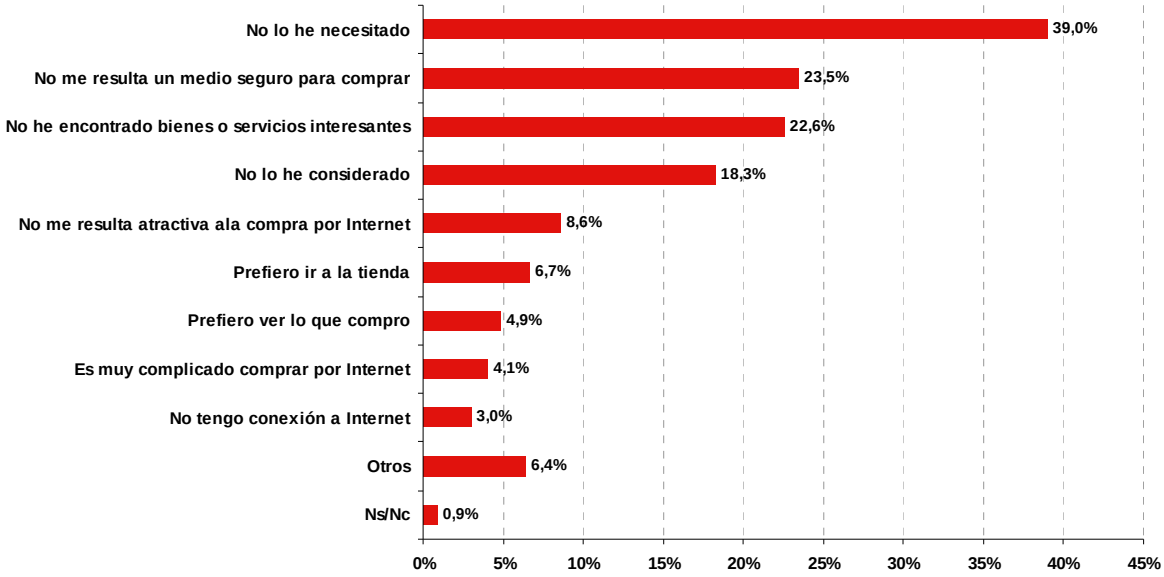


Fuente: INTECO

En el otro extremo, como servicios con una menor frecuencia de uso destacan: los pagos por Internet (transferencias realizadas para el pago de subastas, donativos, u otro tipo de servicios mediante sistemas específicos habilitados al efecto), los *blogs* o diarios electrónicos y la videoconferencia, que no obstante son utilizados por 1 de cada 5 usuarios.

La razón para que sólo uno de cada dos usuarios de Internet no haya utilizado un servicio de compra online se muestra en el Gráfico 33 correspondiente al "Estudio sobre Comercio Electrónico B2C 2006" elaborado por Red.es. Así, aunque la respuesta más generaliza para no realizar compras online es el no haber necesitado usar este tipo de servicio (39,0%), existe un importante grupo de usuarios de Internet (23,5%) que afirman no hacer compras en Internet por no considerarlo un medio seguro.

Gráfico 33: Razones para no comprar en Internet. Año 2006 (%)



Fuente: Red.es

Además de los efectos negativos del *phishing* como freno al desarrollo de la economía basada en transacciones electrónicas y a la desconfianza que se genera por parte de los usuarios de Internet respecto a los sistemas de seguridad; se debe señalar el efecto negativo que para las entidades financieras – como principales entidades afectadas por el fenómeno – supone la pérdida de tiempo empleado en solventar el ataque y los problemas ocasionados[48]

[48] Según el Grupo de Investigaciones de Interés Público de California, además de las perdidas directas por una estafa online o un robo de identidad, las víctimas de estos ataques gastan en promedio 175 horas investigando y dando seguimiento al delito y 23 meses corrigiendo y controlando sus informes de crédito.

3 RESULTADOS CUANTITATIVOS DE LA INVESTIGACIÓN: ESTADÍSTICAS SOBRE EL FRAUDE A TRAVÉS DE INTERNET PARA LOS USUARIOS ESPAÑOLES

Las datos estadísticos sobre fraude online que se muestran a continuación corresponden a la parte cuantitativa de los trabajos de investigación del Estudio. **Es importante señalar que todos los datos de los resultados que se muestran en este capítulo tienen su base en opiniones y percepciones de los usuarios encuestados.**

Los trabajos han comprendido la realización durante el mes de abril de 2007 de 3.076 encuestas a usuarios habituales[49] de Internet de toda España, seleccionados mediante una metodología robusta como puede observarse en la ficha técnica en el epígrafe 1.3 Diseño metodológico. De este modo, con este Estudio, INTECO suple la ausencia datos estadísticos independientes, contrastados y robustos sobre el fenómeno del fraude a través de Internet en España, realizadas sobre una muestra de usuarios amplia y representativa. Asimismo, junto a los datos sobre *phishing*, se obtienen por primera vez cifras sobre prácticas de reciente aparición como, por ejemplo, el *vishing*, o *smishing*.

Complementariamente, el Instituto, consciente de la importancia que el fraude online tiene en la e-confianza de los ciudadanos, a través de su Observatorio, trimestralmente volverá a realizar esta encuesta, de manera que puedan obtenerse series estadísticas que permitan un análisis de la evolución del fenómeno, para con ello servir de apoyo a la elaboración, seguimiento y evaluación de políticas públicas en este ámbito.

En el Gráfico 34 puede observarse como el término "*phishing*" dice ser conocido por un 41,2% de los usuarios de Internet españoles, sin embargo, otros tipos de fraude apenas son identificados. Así, por ejemplo, un 21,6% de los usuarios de Internet afirman conocer qué es el "*scam*", mientras que el "*pharming*" (8,1%), el "*vishing*" (4,1%) y el "*smishing*" (3,7%) apenas resultan familiares para los usuarios españoles con un uso habitual de la Red.

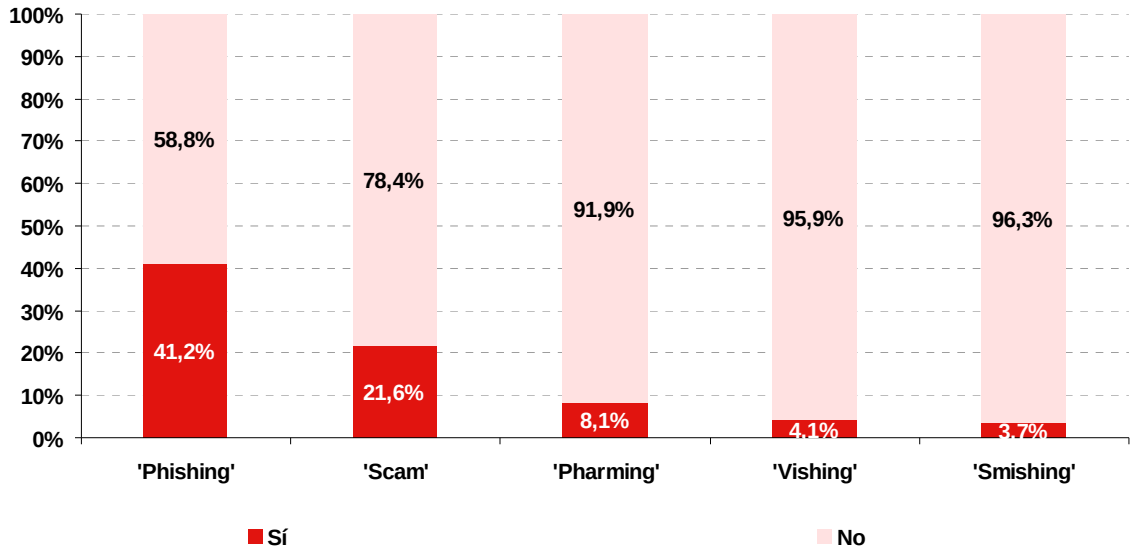
A la vista de estos datos se puede afirmar que más de la mitad de los usuarios de Internet españoles no identifican el término *phishing* como un tipo de fraude online. Este hecho pone de manifiesto el desconocimiento que tienen los usuarios españoles sobre algunas de las prácticas delictivas que se producen a través de la Red y lo importante que es realizar campañas de formación y concienciación entre los propios usuarios para reducir la incidencia de este problema.

[49] Entendiendo como habituales, aquellos que se conectan a la Red al menos una vez al mes.

En este sentido debe reflexionarse sobre la conveniencia de comenzar a utilizar una nomenclatura propia en la lengua española y no inglesa, para que ese proceso de familiarización sea más fluido y sencillo.

Esta idea se apoya en el hecho de que un número significativo de usuarios es consciente del fenómeno fraudulento o incluso lo ha sufrido personalmente, pero no lo identifica con el nombre que desde los medios y la doctrina se viene utilizando.

Gráfico 34: Nivel de conocimiento declarado sobre términos relacionados con el fraude online. (%)



Phishing: Acto de adquirir fraudulentamente información sensible de carácter personal de forma online.
Scam: Oferta de trabajo online *de carácter fraudulento.*
Pharming: Evolución tecnológica del phishing que se concreta en el envenenamiento del sistema DNS (Domain Name Service).

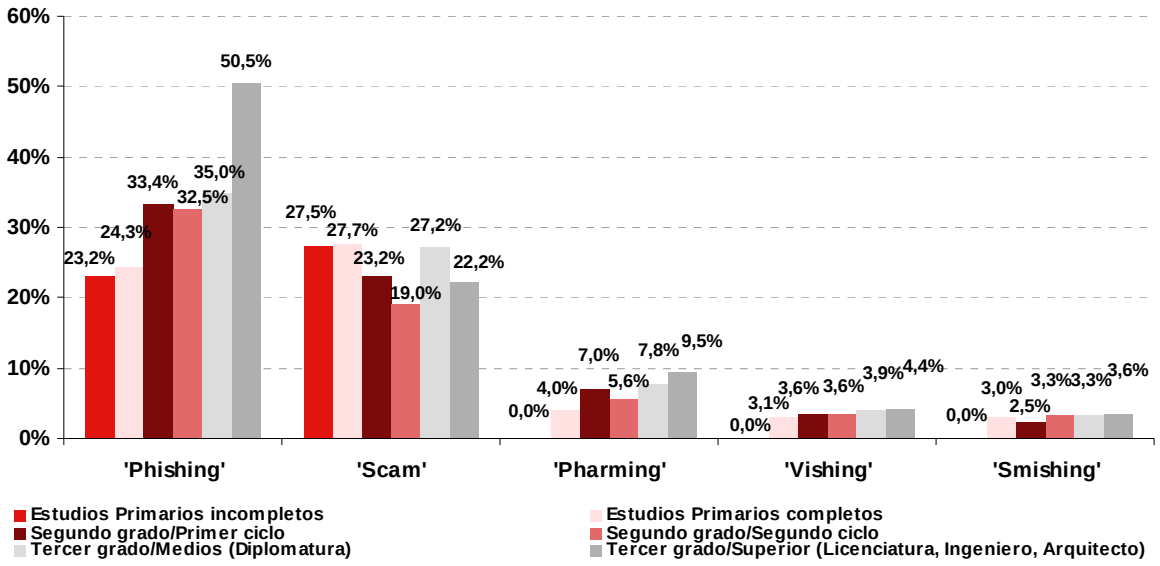
Smishing: Tipo de phishing telefónico que utiliza los mensajes sms de los teléfonos móviles.
Vishing: Tipo de phishing telefónico que utiliza voces grabadas para solicitar los dígitos y la fecha de caducidad de las tarjetas de crédito, produciéndose a continuación las operaciones fraudulentas.

Fuente: INTECO

El Gráfico 35 muestra los datos del nivel de conocimiento declarado de los distintos conceptos en función del nivel de estudios. El *phishing* sigue siendo el término más conocido para todas las categorías analizadas, superándose el 50% en el caso de usuarios pertenecientes al nivel de estudios de grado más alto.

Es significativo que un porcentaje importante del grupo de usuarios con menor nivel formativo conozca las principales modalidades de fraude online que enlazan directamente con el empleo del engaño (un 23,2% para el caso del *phishing* y un 27,5% para el caso del *scam*) y sin embargo, no conozcan ninguno de los otros tres tipos de estafa más relacionados con el empleo de código malicioso (*pharming*) o con la utilización de otros canales que no sea el ordenador (*vishing* y *smishing*).

Gráfico 35: Nivel de conocimiento declarado sobre términos relacionados con el fraude online según nivel de estudios. (%)

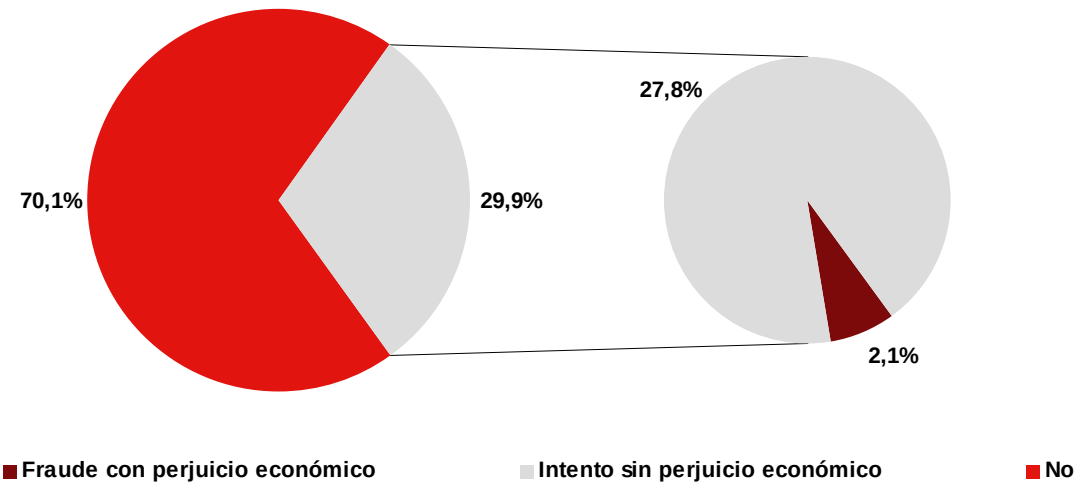


Fuente: INTECO

Llama la atención que la categoría referida al *scam* recoja cifras elevadas para todos los niveles de estudios. Este dato podría deberse a una confusión que cabría considerar como razonable por la similitud en cuanto a su pronunciación y escritura con el término *spam* (correo no deseado) que, de igual manera, se relaciona con el campo de la seguridad informática. Este hecho refuerza la idea anteriormente planteada respecto a la necesidad de que paulatinamente se sustituyan dichos términos anglosajones por otros en nuestro idioma.

El Gráfico 36 muestra como el 29,9% de los usuarios reconocen haber sufrido algún intento de fraude online, aunque sólo reconocen haber sufrido un perjuicio económico el 2,1% de los usuarios españoles de Internet. **En este punto, conviene recordar que los datos de los resultados obtenidos sobre el porcentaje de usuarios que han recibido algún intento de fraude online y el porcentaje de fraude con perjuicio económico se han obtenido a partir de las opiniones de los propios usuarios a través de una encuesta diseñada para este fin. Estos datos se basan en percepciones de los propios usuarios.**

Gráfico 36: Porcentaje de usuarios que han recibido algún intento de fraude online y porcentaje de fraude con perjuicio económico



Fuente: INTECO

Como se ha expuesto en el epígrafe 2.4.2 "El impacto económico y social del *phishing*" de los resultados del trabajo de campo de este estudio se ha obtenido la cifra 593€ como daño medio por cada caso de fraude online en España.

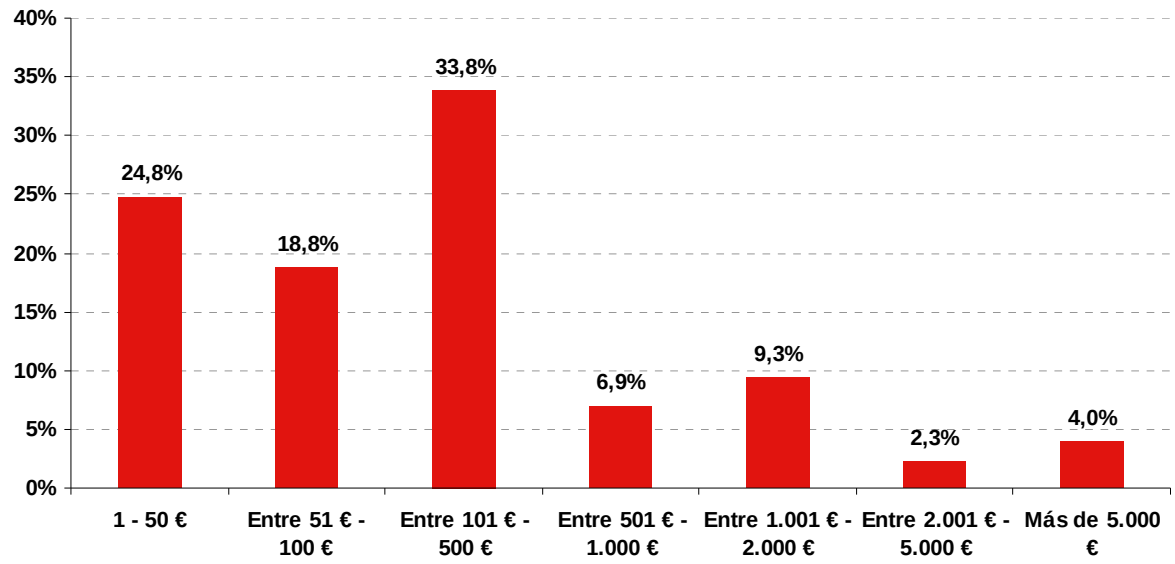
No obstante, en la mayoría de los casos – algo más de 2 de cada 3 fraudes[50] online – el perjuicio económico no supera los 400€. Más aún, la cuarta parte de los mismos es inferior a los 50€. Así, el Gráfico 37 muestra como más del 75% de los fraudes son de una cuantía no excesivamente elevada (menos de 500€) y un 24,8% no alcanzan los 50€.

[50] Al igual que sucede con el valor medio, el porcentaje de fraudes que constituyen falta puede sufrir una variabilidad significativa entre muestras sucesivas. El número de individuos muestrales que reconocen haber sufrido un perjuicio económico con origen en un fraude online es pequeño: de los 3.076 individuos encuestados, únicamente 65 declaran haber sufrido un perjuicio económico.

Este hecho – la relativa escasa cuantía de los fraudes – contribuye a que en muchas ocasiones los fraudes no sean detectados por el usuario al camuflarse entre los apuntes bancarios corrientes, y por tanto no sean conocidos ni denunciados.

Del mismo modo, ha de considerarse que, precisamente ese perjuicio moderado y en muchos casos poco significativo, hace que en numerosos casos las víctimas, aun conociendo la estafa, minimicen el ilícito y decidan no poner el hecho en conocimiento de las autoridades.

Gráfico 37: Porcentaje de usuarios que han sufrido fraude online según perjuicio económico soportado. (%)



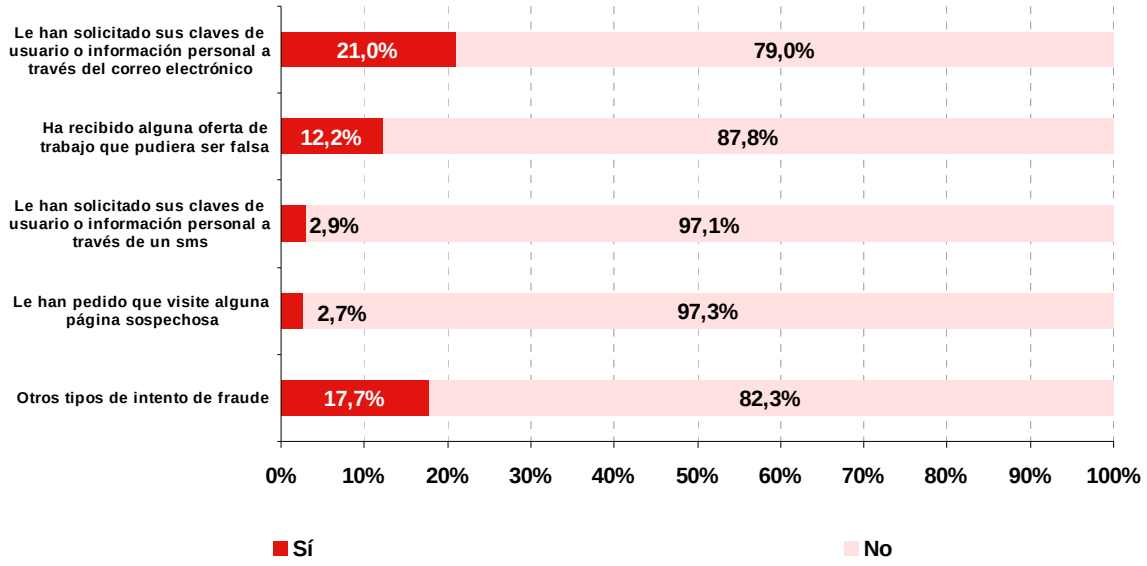
Fuente: INTECO

El porcentaje de usuarios que han sufrido un perjuicio económico puede parecer bajo, sin embargo, multiplicándolo por el número creciente de usuarios de Internet en España, y la cantidad media que supone el fraude (593 €), puede apreciarse la verdadera dimensión del problema.

En otro orden de cosas, en el Gráfico 38 puede observarse de forma desagregada como al menos un 21,0% de los encuestados han sufrido intentos de *phishing*, habiendo recibido un correo electrónico que les solicitaba sus claves de usuario u otra información personal. A este porcentaje podría sumarse el del 2,7% de usuarios que reconocen haber recibido un correo para que visiten una página sospechosa.

Por otro lado destaca el dato que muestra que el fenómeno del *smishing* comienza a tener una incidencia significativa. Así el 2,9% de los usuarios de Internet españoles declaran haber sido objeto de un intento de fraude a través de un mensaje corto recibido en su teléfono móvil (sms)

Gráfico 38: Porcentaje de intentos de fraude sufridos por los usuarios de Internet españoles según tipología.

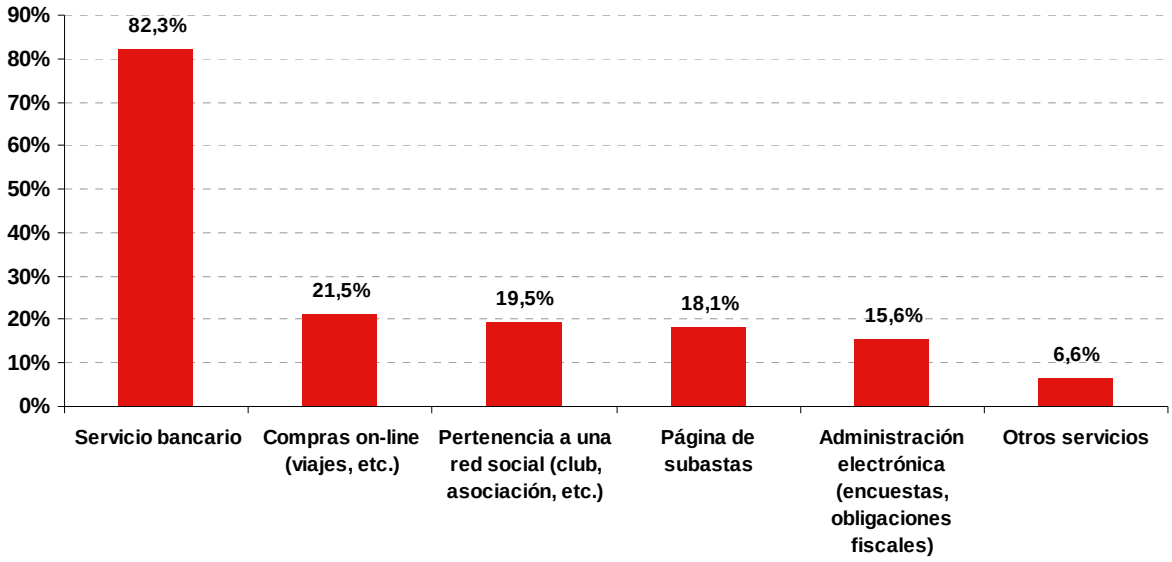


Fuente: INTECO

Analizando los datos de correo electrónico no deseado (*spam*) y de *phishing* que se han detallado a lo largo del Estudio, junto con el conocimiento del fraude online y el nivel declarado de incidencias, se puede concluir que la falta de formación hace que gran parte de los usuarios españoles de Internet no identifiquen de manera adecuada los intentos de fraude de los que son objeto a través de correo electrónico.

El Gráfico 39 muestra como el principal objetivo de los intentos de *phishing* son los servicios bancarios. De esta forma un 82,3% de los usuarios que han sufrido un intento de fraude en el que se le solicitaban claves personales, declaran que las claves solicitadas correspondían a las contraseñas de acceso a su servicio bancario. A bastante distancia aparecen otro tipo de claves solicitadas: de sitios de compras online (21,5%), de asociaciones o redes sociales (19,5%), de páginas de subastas (18,1%) y de servicios de administración electrónica (15,6%).

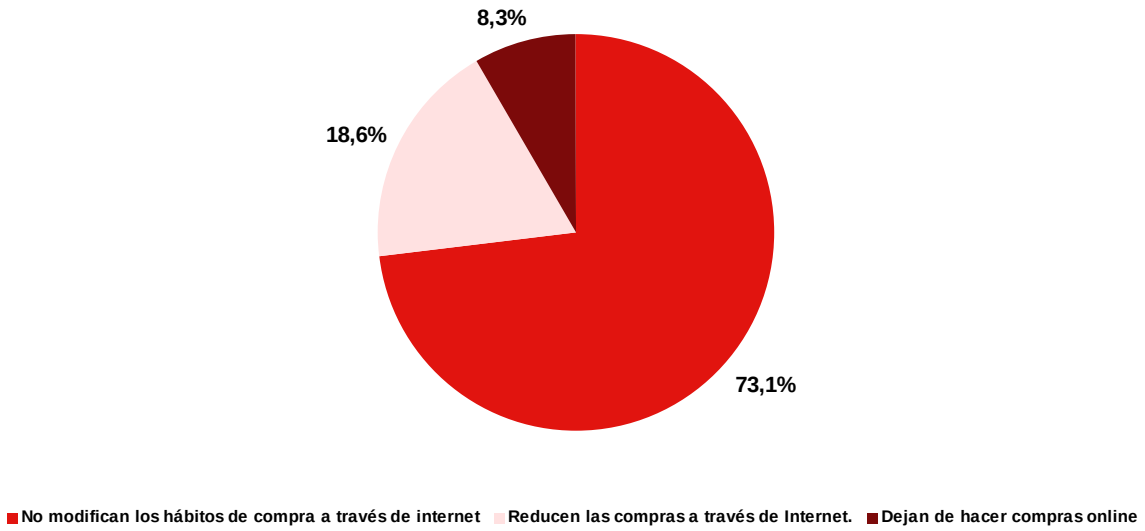
Gráfico 39: Tipología de los servicios online de los que solicitan claves personales a los usuarios españoles que han sufrido un intento de fraude (%)



Fuente: INTECO

En el Gráfico 40 se analizan las variaciones de comportamiento respecto de los servicios de compra online de los usuarios españoles de Internet tras haber sido objeto de un intento de fraude. Sólo uno de cada cuatro usuarios modifican sus hábitos de compra tras haber sufrido un intento de fraude: en concreto, un 18,6% de los usuarios han reducido las compras tras el intento de fraude y un 8,3% han dejado de realizarlas.

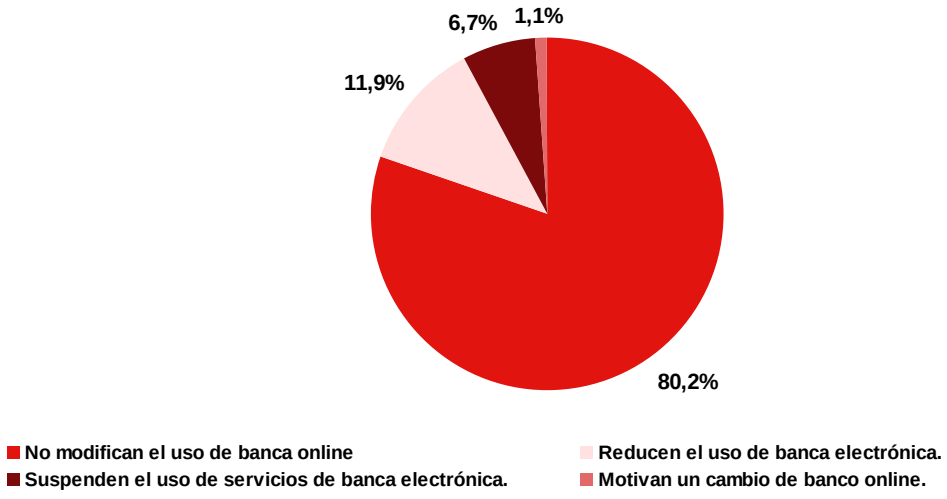
Gráfico 40: Variación en los hábitos de compra online de los usuarios de Internet españoles que han sido objeto de un intento de fraude (%)



Fuente: INTECO

Como se aprecia en el Gráfico 41, la variación en los hábitos de uso de la banca a través de Internet es similar a la que se produce respecto a las compras de comercio electrónico.

Gráfico 41: Variación en los hábitos de uso de la banca online de los usuarios de Internet españoles que han sido objeto de un intento de fraude (%)



Fuente: INTECO

Así, menos de un 20% de los usuarios modifican su comportamiento tras haber sufrido un intento de fraude. Sólo el 6,7% dejan de usar el servicio de banca electrónica, y un 11,9% lo reducen.

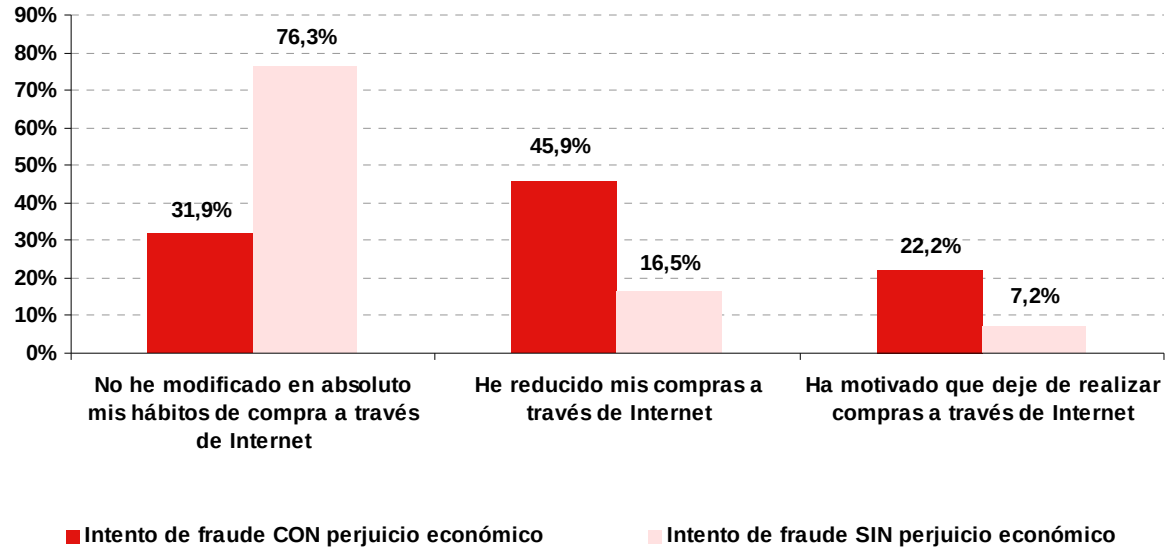
La causa de que un 80,2% de usuarios de banca online no modifiquen su comportamiento a pesar de la sensación de inseguridad que puede provocarles recibir intentos de fraude se debe a que, en general, los usuarios habituales de Internet han asumido de tal forma los servicios bancarios a través de Internet en su estilo de vida que se les hace muy difícil prescindir de los mismos. Así, las incidencias sufridas no se interpretan como razones para reducir o abandonar el uso de estos servicios. Esta idea se ve reforzada cuando se compara la variación en los hábitos de uso de los usuarios de Internet de comercio (Gráfico 40) y banca (Gráfico 41) tras haber sido objeto de un intento de fraude.

Así, para el servicio de banca electrónica la alteración de hábitos es menor con un 19,7% (Gráfico 41) frente al 26,9% (Gráfico 40) de variación en los hábitos del servicio de compra online, y es que el servicio de banca online no sólo está más extendido entre la población y por tanto más consolidado, sino que las ventajas operativas del propio servicio – con unas condiciones de prestación más cómodas (horarios, comisiones, información, etc.) que la banca tradicional, que no siempre se dan en la compra online – hacen que el usuario de banca electrónica a pesar de haber sufrido un intento de fraude, valore mucho más las ventajas del servicio que renunciar al mismo.

Por otro lado, es significativo, que únicamente un 1,1% de los usuarios optan por cambiar de banco, esto es, ante un intento de fraude un porcentaje bastante reducido de los usuarios culpabiliza a su proveedor de servicios bancarios de una posible falta de medidas de seguridad.

En el Gráfico 42 se muestran las diferentes actuaciones de los usuarios en el caso de haber sufrido sólo un intento de fraude, y en el caso de que este fraude se haya llevado a término.

Gráfico 42: Variación en los hábitos de compra online de los usuarios de Internet españoles, en función de la existencia o no de perjuicio económico (%)



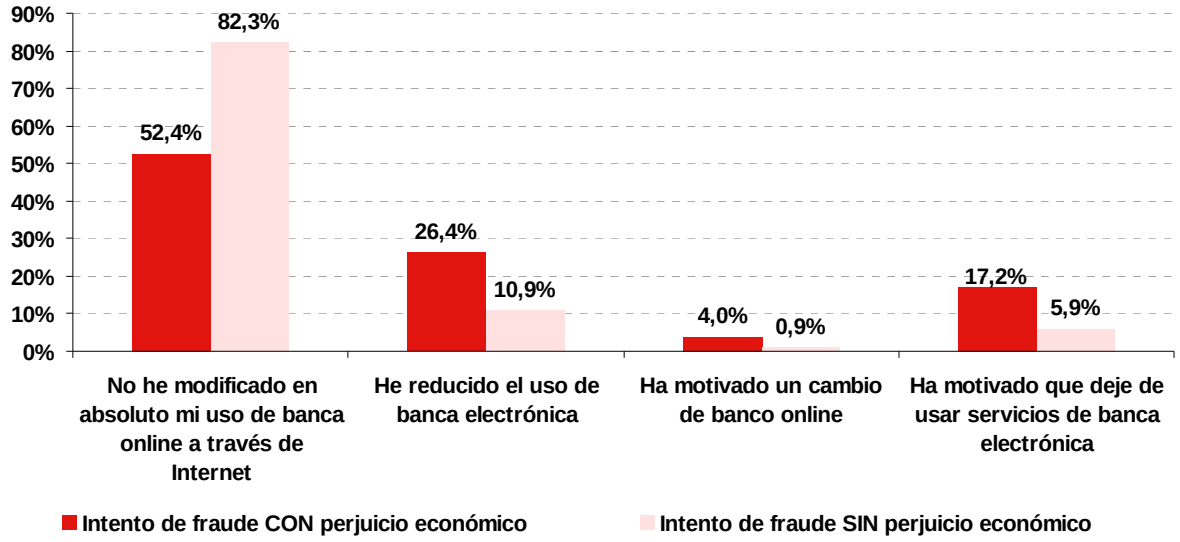
Fuente: INTECO

Como puede observarse en el caso de que los usuarios hayan sido victimas de un fraude con perjuicio económico la tendencia se invierte, y sólo un tercio de los afectados mantienen invariables sus hábitos de compra online. Por el contrario, el porcentaje de usuarios que dejan de realizar compras online tras sufrir un fraude con perjuicio económico, triplica, con un 22,2%, al de usuarios que no han sufrido perjuicio económico (7,2%).

Con el servicio de banca online sucede algo similar, como puede verse en el Gráfico 43. Sin embargo, en este caso, la mitad de los usuarios que han sufrido fraude con perjuicio económico no modifican sus hábitos y uno de cada cuatro reduce el uso del servicio.

En este sentido, señalar que, como se indicaba en el Gráfico 39, al 82,3% de las personas objeto de fraude se les han requerido sus claves bancarias, frente a un 21,5% que declaraban que se les había solicitado las claves de sus servicios de compra online. Lo que da a entender que los intentos de fraude son más frecuentes en el caso de los servicios bancarios. Sin embargo, paradójicamente, una vez que el fraude es efectivo los primeros servicios en abandonarse son los servicios de compra online.

Gráfico 43: Variación en los hábitos de uso de la banca online de los usuarios de Internet españoles, en función de la existencia o no de perjuicio económico (%)



Fuente: INTECO

Los servicios de banca online, a pesar de concentrar la mayor parte de los intentos de fraude, no se abandonan de manera inmediata. Así, los usuarios prefieren tomar una serie de medidas previas para evitar incidencias futuras en lugar de volver a utilizar el método tradicional. La razón puede ser doble: de un lado, una mayor e-confianza en los prestatarios de los servicios – las entidades financieras –, y de otro lado, la irrenunciabilidad del servicio.

4 POSICIONAMIENTO Y PAPEL DE LOS AGENTES AFECTADOS POR EL FENÓMENO DEL *PHISHING*

En el mundo físico cualquier sujeto, de manera individual o formando parte de una organización (empresa o administración) puede resultar víctima de un acto delictivo de carácter fraudulento. Esta situación de riesgo trasladada a la Red acecha de igual manera a los mismos sujetos (usuarios, empresas y administraciones) y en la misma forma (ya sea individual o colectivamente como parte integrante de las organizaciones).

En este capítulo se define el papel de los agentes afectados y a la vez intervinientes en el ámbito de desarrollo del fenómeno del *phishing*, describiendo las medidas de actuación que cada uno de ellos, bien de forma individual o en conjunto, desempeñan a lo largo del proceso.

4.1 Las entidades financieras y otras empresas prestadoras de servicios a través de Internet

Las empresas que operan a través de Internet son los agentes más relevantes para promover la seguridad de las transacciones electrónicas, ya que la reducción del fraude en Internet es una de sus principales preocupaciones puesto que afecta a su modelo de negocio.

En este sentido, algunas empresas se han lanzado a “competir en seguridad”. Este es un hecho positivo, ya que supone una lucha constante por incrementar los niveles de seguridad para sus clientes, implementando medidas cada vez más avanzadas.

Además, existen diversas iniciativas, lanzadas a través de plataformas creadas por empresas o por servicios comunes a éstas, que tratan de promover la seguridad informática, que han realizado diferentes actuaciones contra el *phishing*.

Desde un punto de vista amplio, la **Organización Internacional para la Estandarización** (www.iso.org) ha creado una norma acerca de la seguridad de los Sistemas de Información, denominada **ISO 17799**, que trata de **recopilar las mejores prácticas empresariales en este terreno aplicables a toda empresa, sea cual sea su tamaño o sector.**

En un terreno más específico, quizá la iniciativa más amplia a escala global para la prevención del *phishing* es el **Anti-Phishing Working Group (APWG)**. Este grupo de trabajo desarrolla diversos tipos de iniciativas divulgativas para dar a conocer la importancia del *phishing* y frenar sus efectos entre la población. Su página, www.anti-phishing.org, es un centro de información completo y actualizado sobre todo tipo de engaños a través de la Red, y muy especialmente sobre el *phishing*. Alertas, consejos,

denuncias y contactos son algunas de las funcionalidades que proporciona esta organización.

Con el fin de incrementar el conocimiento en torno a este fraude, el APWG organiza congresos para tratar de analizar desde una perspectiva científica las últimas tendencias, y extraer conclusiones y recomendaciones valiosas. Por otro lado, sus informes sobre la situación del *phishing* son punto de referencia necesario en el estudio de este fenómeno a escala global.

El **Foro Abuses** (www.rediris.es/abuses) es una iniciativa que reúne a algunas de las organizaciones profesionales que tienen que trabajar diariamente para evitar los impactos y las amenazas sobre los sistemas de información. Sus objetivos principales están relacionados con la lucha contra los abusos informáticos, como son el correo no deseado (*spam*), los códigos maliciosos, los ataques a sistemas informáticos o las violaciones de derechos de propiedad intelectual.

Las organizaciones participantes en este foro intercambian información sobre la procedencia de los ataques, los medios utilizados y, en general, todos los datos que puedan resultar útiles para combatir cada ataque. De este modo, colaboran para eliminar las amenazas lo antes posible y minimizar su impacto, ya que este intercambio de información facilitará la detección del estafador y el cierre de los sitios web desde los que se producía el fraude.

Este foro, participado por empresas privadas, es también muestra de la preocupación de los poderes públicos, que han contribuido a su promoción a través de **RedIris** (www.rediris.es), la Red de información que aglutina a diferentes centros de conocimiento e investigación.

La cooperación de este foro se produce también a escala europea a través de ***European Cooperation of Abuse Fighting Teams* - E-COAT-** (www.e-coat.org) algo muy importante dado que el problema de la seguridad tiene, como ya se ha visto, dimensión global.

La industria de la seguridad informática es uno de los grandes agentes relacionados con la prevención de los fraudes electrónicos. Casi todas las empresas fabricantes de software relacionado con la seguridad informática llevan a cabo diferentes iniciativas, a veces en colaboración con las autoridades, para valorar y difundir el impacto de las amenazas cibernéticas en la sociedad.

Algunas de estas organizaciones han creado la **Ciber Security Industry Alliance** (www.csialliance.org) destinada a colaborar en la lucha contra la delincuencia informática y mejorar los estándares de seguridad existentes. Esta organización elabora un informe sobre la confianza en Internet.

Finalmente, es interesante comentar la iniciativa de **A.P.A.C.S.**, la asociación británica de medios de pago (www.apacs.org.uk), por cuanto se trata de una actuación realizada por parte de algunos de los principales perjudicados. Posiblemente por ello, evitando posibles recelos al actuar de manera cooperativa, esta asociación elabora diferentes informes sobre la magnitud de los diferentes tipos de estafas bancarias, entre las que se encuentran los fraudes de tarjetas de crédito, los cheques falsos y el *phishing*.

4.1.1 Bancos, cajas de ahorros y cooperativas de crédito

Aun existiendo, igualmente, otras empresas y organizaciones afectadas por suplantaciones fraudulentas de sus sitios web: casas de subastas, sitios de donaciones a ONG´s, incluso organismos públicos (INE, AEAT, etc.) quizás los casos más paradigmáticos de *phishing* se producen en los servicios de banca online de las entidades financieras.

Desde el primer momento estas organizaciones han incorporado a su modelo de negocio la utilización de Tecnologías de la Información acercando sus servicios a sus clientes. Esta mejora del servicio para los clientes, ha sido objeto de ataques por los delincuentes informáticos con la finalidad de apropiarse ilegítimamente de beneficios económicos. El sector bancario en España está adoptando un comportamiento ejemplar. Una vez que saben que un cliente ha sufrido un fraude en su cuenta a través de Internet, están asumiendo el coste que conlleva el daño producido.

En todo caso, el interés de las entidades financieras es doble y recae, de un lado, en que sus clientes conozcan y tomen las medidas de seguridad más oportunas para evitar que se produzca cualquier tipo de fraude a través de la Red y, de otro, en lo que respecta a la propia Entidad, con el objeto de activar todos los mecanismos de seguridad necesarios para prevenirlo.

Medidas de actuación individuales

Ante esta situación y con el fin último de prevenir los ataques de *phishing*, las entidades financieras están adoptando las siguientes medidas de actuación:

a) La contratación de servicios especializados de empresas de seguridad informática.

b) La creación de un departamento interno de seguridad informática, con la función de estudiar y detectar posibles páginas falsas y, en general, cualquier tipo de código malicioso.

Ambas opciones reducen notablemente la incidencia de este tipo de acciones fraudulentas, por lo que la toma de decisiones para la adopción e implantación de una u otra medida recae de manera particular en cada entidad financiera.

Medidas de actuación conjunta

Este sistema individualmente elegido se complementa con otras medidas de actuación conjunta en materia de seguridad informática. Para este cometido, el Centro de Cooperación Interbancaria (CCI) – www.asociacioncci.es – ha establecido entre sus ***grupos de trabajo*** uno específico destinado al estudio de la seguridad informática. El objetivo de estos grupos es que las entidades de depósito (Bancos, Cajas de ahorros y Cooperativas de crédito) compartan información y estrategias.

Estos grupos establecen una serie de protocolos que indican las acciones a realizar en el caso de que alguno de los miembros reciba un ataque, incluyendo normas para realizar las devoluciones a los clientes afectados.

De la colaboración de estos grupos ha surgido una definición del ciclo del fraude que se conforma en las siguientes ocho fases:

1. Disuasión
2. Prevención
3. Detección
4. Mitigación
5. Análisis
6. Investigación
7. Instalación de políticas
8. Persecución

En línea con lo anterior, y para minimizar el fraude electrónico, el **Grupo de Trabajo de Seguridad Informática del Centro de Cooperación Interbancaria (CCI)** trabaja en la puesta en marcha de diferentes servicios en los que se hace partícipe a los sujetos intervinientes en el proceso del fraude a través de Internet, en cada una de sus parcelas de actuación:

1. Implementación de un sistema que dificulte el registro de marcas similares a otras reconocidas (Foro de Marcas Renombradas) [51] o de marcas notorias debidamente inscritas en la Oficina Española de Patentes y Marcas, así como cualquier variación de las mismas que pueda llevar a confusión a un usuario.

2. Realización de los cambios oportunos en el Procedimiento de Cancelación de dominios establecido por Red.es, con la finalidad de agilizar los trámites de cancelación en el caso de nombres de dominios ".es" ya registrados por terceros, que sean coincidentes o similares a marcas reconocidas o marcas notorias debidamente inscritas.

[51] El Foro de Marcas Renombradas Españolas es la iniciativa de un grupo de empresas líderes en distintos sectores, que cuentan con marcas destacadas con sostenida implantación internacional y vocación de permanencia en los mercados exteriores, que se unen con el fin de trabajar en el desarrollo, la defensa y la promoción de las Marcas Renombradas Españolas. Más información en www.marcasrenombradas.com

3. Habilitación de mecanismos de aviso a las entidades, del intento de registro o del registro de nombres de dominio que sean variaciones de sus marcas reconocidas con el fin de que éstas puedan ejercer de forma eficaz sus legítimos derechos.

4. Establecimiento – conjuntamente entre las administraciones y las entidades financieras – de un procedimiento ágil que facilite solicitar el bloqueo de cualquier dominio ".es" utilizado para fines fraudulentos.

En abril de 2007 el CCI anunciaba la puesta en marcha de un sistema integral de prevención del fraude (robos de identidad, delitos electrónicos, clonación o robos de tarjetas) para el sector financiero. Esta iniciativa denominada **Servicio de Prevención del Fraude (SEPFRA)**[52] incluye entre sus actividades:

- La creación del **Centro de Observación del Delito Económico (CODE)** formado por un grupo de expertos en análisis, seguimiento y detección temprana de tendencias y técnicas de comisión de fraude. Entre los servicios que prestará este observatorio a las entidades adheridas se encuentran el envío periódico de estadísticas y análisis, acceso permanente a un completo centro de documentación actualizado, programas de formación para empleados y envío de alertas tempranas relacionadas con el fraude.

  Además pondrá a disposición de los consumidores una página web con información sobre distintos delitos económicos, su incidencia y evolución, técnicas de comisión más habituales, y consejos prácticos de protección personal.

- El establecimiento de **acuerdos de colaboración** con instituciones y organizaciones públicas y privadas implicadas en la lucha contra el delito económico, tanto a nivel nacional como internacional.

4.2 Los fabricantes y proveedores de servicios de seguridad informática

La principal labor de las empresas de seguridad informática consiste en ofrecer productos y prestar servicios de soporte a las empresas, usuarios y administración para mejorar su seguridad.

En este sentido, se puede considerar que trabajan en dos frentes con mayor intensidad:

- La prevención del fraude: Las compañías tratan de detectar cualquier tipo de código malicioso susceptible de ser utilizado con una finalidad fraudulenta (troyanos bancarios, capturadores de pulsaciones) antes de que se difundan en

[52] http://www.experian.es/apartados/salaprensa/noticias/NP_Lanzamiento%20Sepfra_26apr07.pdf

la Red y ofrecen tanto métodos de detección y prevención, como soluciones a incidencias e infecciones. Asimismo, desarrollan parches de seguridad minimizando las posibles vulnerabilidades que acontezcan en sus sistemas operativos y programas informáticos. Por otro lado, prestan servicios a las propias entidades financieras con sistemas de filtrado del tráfico, de protección ante intrusiones, detección de webs fraudulentas, etc.

- La investigación e innovación tecnológica: Las compañías de seguridad realizan una labor de apoyo en la investigación, colaborando con otros agentes implicados como son los Cuerpos y Fuerzas de Seguridad del Estado.

Como se ha señalado, entre sus principales clientes se encuentran las entidades financieras, las empresas de venta de productos online y las empresas de subastas a través de Internet. Su principal fortaleza está en adelantarse a la estafa, localizando "dominios primos" o cualquier otro tipo de web fraudulenta para bloquearla y minimizar el posible daño.

A la hora de recoger las medidas específicas aplicables a las empresas, conviene nuevamente recordar la existencia del doble origen del riesgo. De un lado, el origen de dicho riesgo pueden ser los fallos de seguridad y vulnerabilidades de los propios sistemas y aplicaciones informáticas utilizados por las empresas; y de otro lado, es evidente el riesgo derivado del engaño a los usuarios, que pueden caer en trampas de ingeniería social y revelar información confidencial a estafadores que posteriormente suplanten ilegítimamente su identidad. Una vez identificado y cuantificado el riesgo de fallos o vulnerabilidades en los sistemas, es necesario establecer las medidas o salvaguardas de seguridad administrativas, físicas y técnicas acordes al nivel de riesgo que aseguren un nivel de control adecuado.

Las salvaguardas técnicas son controles que se implantan a través de soportes físicos o lógicos Entre ellas se incluyen antivirus, herramientas de gestión de red, firmas digitales, cifrado, contraseñas, tarjetas inteligentes, seguimiento de huellas o trazas de auditoría y sistemas expertos de detección de intrusiones.

Las salvaguardas son dispositivos físicos o lógicos difíciles de vencer y capaces de reducir el riesgo de materialización de una amenaza y que, una vez implantados, pueden funcionar sin la intervención humana,. Existen dos tipos: *salvaguardas de carácter preventivo*, aquellas destinadas a impedir la materialización del impacto o, al menos, reducir su probabilidad; *y salvaguardas curativas o protectoras*, destinadas a reducir el impacto una vez se ha producido.

Con la adopción de estas salvaguardas, y ante un posible intento de *phishing*, las empresas intentarán evitar que llegue a causar ningún efecto sobre sus sistemas o

usuarios; y en caso de que éste se produzca, tratará de articular respuestas tempranas para limitar este impacto, reduciendo, entre otras cosas, el tiempo de exposición.

Para reducir vulnerabilidades, algunas organizaciones han comenzado a implantar diversas herramientas técnicas que tratan de garantizar la seguridad del sistema.

Así, los datos recogidos en el *Estudio sobre seguridad y e-confianza en las Pymes españolas* del Observatorio de la Seguridad de la Información de INTECO[53] los datos recogidos en el Gráfico 44 reflejan como principal medida de protección utilizada por las empresas españolas la alta implantación de los sistemas antivirus. Los cortafuegos, los programas anti-correo no deseado y anti-espía superan el nivel medio dentro de las medidas de protección instaladas en los equipos de las empresas españolas. Por último, el cifrado de las comunicaciones con casi un 27% es la medida de seguridad menos significativa adoptada por las empresas españolas.

Gráfico 44: Porcentaje de utilización de medidas de seguridad en las empresas españolas en 2007

Fuente: INTECO (2007)

Aunque la utilización de antivirus, cortafuegos y sistemas de detección de las intrusiones, a través de herramientas más completas que las disponibles para los usuarios domésticos, es un punto de partida necesario para las organizaciones, puede no resultar del todo suficiente, para obtener la seguridad del sistema de información.

[53] En elaboración.

Por lo anterior, muchas compañías están avanzando en la utilización de sistemas técnicos más robustos. En este sentido, y dado que uno de los problemas más habituales proceden de la identificación a través de la utilización de un único sistema de identificación, la línea básica de actuación ha sido la utilización de sistemas que requieran varios métodos simultáneos de identificación, de modo que el delincuente debe tener acceso a todos ellos si desea poder ejecutar su ataque.

No obstante, si todos los elementos de identificación tienen la misma naturaleza, el grado de exposición sería prácticamente el mismo, ya que sólo se requeriría el robo de unos pocos bits más de información por parte del criminal.

En este sentido, lo más común es añadir al método de identificación inicial un segundo requisito necesario que, en principio, sólo pueda estar en manos del usuario autorizado. La idea genérica es bien expresada por Verisign[54]. Son varios los caminos seguidos para ello:

1. **Las contraseñas de un solo uso** (One Time Password u OTP) son códigos de acceso únicos, que se generan cada vez que se desea acceder al sistema por parte de un dispositivo sólo disponible por el usuario. De este modo, si alguien desea suplantarle, necesita disponer tanto de la contraseña alfanumérica estable como del dispositivo que genera las nuevas contraseñas. Sólo un ataque bien articulado a través de un man in the middle que actúe, por ejemplo, como servidor proxy, puede engañar al usuario, que creerá estar operando contra su sistema y no contra el del criminal.

   Este sistema es bastante seguro, y elimina los ataques tradicionales a través del uso simple de ingeniería social. No obstante, uno de sus problemas es la necesidad de llevar físicamente el dispositivo. Si bien son de pequeño tamaño, en el caso de que el usuario requiera acceder a varios sistemas la incomodidad puede ser notable, llegándose a necesitar, como afirma el informe de Verisign, “un collar de tokens”[55].

2. Una variedad del método anterior utiliza las conocidas **tarjetas de coordenadas**. Se trata de una relación de contraseñas organizadas por filas y columnas y única para cada usuario. En este caso se gana en portabilidad, aunque se pierde en seguridad, ya que un usuario poco informado sobre los fraudes en Internet podría llegar a comunicar a los estafadores los valores de su tarjeta, que no se generan en cada ocasión[56].

[54] Informe Verisign: “Mezclar algo que sabes con algo que tienes”.

[55] Pequeños dispositivos con acceso a puerto USB, certificados personales o, en algunos casos, tarjetas inteligentes.

[56] De hecho, se han dado casos en los que el usuario ha remitido esta información por medio de fax al estafador, tras haberse hecho pasar por la compañía y aducir brechas de seguridad.

3. **Las preguntas de desafío** suponen la formulación al usuario de cuestiones cuya respuesta, en principio, debe ser conocida solamente por éste. Una variedad de este método consiste en mostrar en la pantalla de acceso imágenes que sólo el usuario conoce, de forma que si el usuario es redireccionado a otra página que en realidad no pertenece a la entidad a la que se quiere acceder, reconocería la ausencia de estas imágenes.

4. **La utilización de dispositivos o elementos identificadores**. En este caso, el dispositivo no genera una contraseña cada vez que se utiliza, sino que simplemente identifica al usuario, ya que sólo le pertenece a él. En este caso, el tipo de dispositivos utilizados vuelven a ser tokens.

   Nuevamente, la seguridad de este tipo de elementos es muy elevada, siendo prácticamente imposibles de burlar, salvo a través de un ataque man in the middle. En su contra, la incomodidad y el incremento en el coste. Por otro lado, el almacenamiento de tarjetas y contraseñas originales debe ser cuidadoso, ya que en ocasiones los usuarios las guardan en un mismo sitio (la cartera), de modo que su robo es algo más sencillo.

5. **Los dispositivos de identificación biométrica**. En algunos de los sistemas de información donde son necesarios mayores requerimientos de seguridad, y con acceso de un número muy limitado de personas, se utilizan este tipo de dispositivos. Requieren del usuario en el momento de acceder al sistema no sólo una contraseña, sino que el propio sistema verifique un determinado rasgo físico perfectamente identificador, (pupilas, huellas digitales, tamaño de la mano, voz,…).

   Obviamente, se trata de las medidas de seguridad más difíciles de burlar, dado que requieren una sofisticación tecnológica y una clara intención de atacar un sistema informático concreto, esto es, no se busca ganar dinero, sino causar un efecto en una organización concreta. Sin embargo, a día de hoy, no parece posible la utilización masiva de este tipo de medidas, por el elevado coste del hardware y la existencia de pocos programas de requerimientos biométricos, salvo, quizás, los programas de reconocimiento de voz disponibles en el mercado.

Quizás la cuestión más importante acerca de la utilización de este tipo de medidas de seguridad, como ya se ha puesto de manifiesto en algunos casos, es la existencia de un equilibrio entre seguridad y comodidad: cuanto más seguro sea el acceso a un sistema de información, más complejidad técnica o acciones por parte del usuario serán necesarias.

En este sentido, las organizaciones tienen una doble tarea: por un lado, encontrar el equilibrio adecuado entre seguridad y facilidad de uso; y por otro, realizar un trabajo pedagógico, que convenza a sus clientes de la importancia de la seguridad, aunque suponga cierta pérdida de comodidad.

Para concluir con los aspectos relativos a la identificación, Verisign, la empresa responsable de la creación de las transacciones seguras vía SSL[57], apuesta por la creación de unos sistemas de identificación avanzados, a los que denomina "Identity 2.0". El funcionamiento de este tipo de sistemas, al que ya se aproximan algunas aplicaciones existentes, sería el siguiente:

- Un individuo que desee realizar transacciones o entrar en determinados sitios web obtiene una identidad, proporcionada por una empresa a la que se podría denominar *identity broker*, agente de identidades. Esta empresa almacena la información del usuario relativa a esa identidad, para que pueda ser utilizada en las transacciones del individuo, y le proporciona formas de identificarse en sus transacciones (siendo válido cualquiera de los medios mencionados).

- Cuando este individuo desee realizar una transacción con otro o con una empresa, ésta solicita al *identity broker* la información pertinente para la transacción a realizar o, en algunos casos, simplemente la confirmación de que el individuo es quien dice ser, con lo que se mantiene la privacidad de la información original.

La transacción, sea de la naturaleza que sea (transferencias de dinero o de información valiosa, acceso a servicios de las administraciones en la Red o, incluso, acceso a comunidades o *blogs*), es realizada exitosamente.

4.3 El Poder Judicial y los Cuerpos y Fuerzas de Seguridad del Estado

La Resolución 55/63 de las Naciones Unidas (acordada en el año 2000), destinada a combatir el uso delictivo de las tecnologías de la información, plantea a los Estados miembros un decálogo de necesidades, que puede ser considerado un catálogo genérico de medidas:

- Los Estados deben asegurarse de que su ordenamiento y práctica jurídicos eliminan los resquicios seguros para los delincuentes informáticos.

- La cooperación entre las Fuerzas de Seguridad de los diferentes países para la investigación y persecución de los delitos informáticos debe ser coordinada entre todos los Estados afectados.

- Los Estados deben intercambiar información acerca de los problemas que afrontan a la hora de combatir los delitos informáticos.

[57] *Secure Sockets Layer*: Protocolo de intercambio de información segura o protocolo criptográfico que proporciona comunicaciones seguras en Internet. Utilizando la técnica criptográfica el certificado SSL proporciona autenticación de los elementos comunicados y privacidad de la información transmitida.

- Las Fuerzas de Seguridad deben estar preparadas, equipadas y formadas para identificar los delitos informáticos.

- Los ordenamientos jurídicos deben proteger la confidencialidad, integridad y disponibilidad de los datos y los sistemas de información frente a los ataques y asegurarse de que los delitos son perseguidos.

- Los ordenamientos jurídicos deben permitir el mantenimiento y el acceso rápido a los datos relativos a investigaciones criminales en curso.

- Los sistemas de cooperación deben asegurar la información rápida de los delitos informáticos y la recopilación y puesta en común inmediata de las evidencias existentes en estos casos.

- Hay que hacer que la opinión pública tome conciencia de la necesidad de prevenir y combatir los delitos informáticos.

- Hasta donde sea posible, las Tecnologías de la Información y las Comunicaciones deben ser diseñadas de forma que permitan prevenir y detectar el uso delictivo, perseguir al criminal y recopilar pruebas.

- La lucha contra la delincuencia informática debe tener en cuenta simultáneamente el respeto a los derechos y libertades de los individuos y la eficacia de los Gobiernos en dicha lucha.

En este sentido, el Estado español aborda su cumplimiento desde posiciones y competencias diferentes. De un lado, las labores de vigilancia, investigación y persecución del fraude se realizan a través de las FCSE y los órganos del Poder Judicial, y de otro, las tareas de prevención, elaboración normativa, sensibilización, formación y divulgación se llevan a cabo a través de los correspondientes organismos de las Administraciones Públicas.

Los Jueces y Tribunales y los Cuerpos y Fuerzas de Seguridad del Estado (CFSE) tienen un papel crucial en el proceso del fraude online, realizando la labor de vigilancia y persecución de las estafas informáticas.

En ambos casos, se han creado grupos especializados con personal altamente cualificado y experimentado en este tipo de delitos informáticos desempeñando las siguientes tareas:

- Labor reactiva: investigación de la procedencia del fraude y persecución y reprensión del autor una vez que se ha cometido.

- Labor proactiva: tarea de carácter preventiva y de vigilancia consistente en el rastreo de la Red en busca de sitios webs de carácter fraudulento que se encuentren activos.

Se ocupan de la tramitación, instrucción y enjuiciamiento de denuncias recibidas directamente por las propias entidades financieras o a través de sus clientes. Asimismo, las empresas de seguridad informática y los organismos como INTECO (a través de su CERT[58]), también les aportan información de valor para la persecución del fraude.

En cada proceso de investigación del fraude a través de Internet, los CFSE avanzan en minorar las barreras inherentes a la especialidad de estos delitos:

- El delito a través de Internet tiene en la mayoría de los casos un carácter internacional o transnacional, que dificulta el seguimiento de los delincuentes. En estos casos es necesaria la actuación de la **Comisión Rogatoria Internacional**. El necesario cumplimiento de estos trámites unido a la rapidez con la que se comete el delito exige un mayor esfuerzo para la captura del delincuente. En Europa Occidental y Estados Unidos existen acciones coordinadas, sin embargo, en otras zonas como Europa del Este y Asia han de mejorarse los mecanismos de coordinación y cooperación.

- Además del carácter internacional o transnacional del delito, la rapidez en la ejecución del mismo dificulta la actuación de los Cuerpos y Fuerzas de Seguridad del Estado. Para evitar esta situación, los CFSE inician de forma ágil el procedimiento para el bloqueo de páginas webs fraudulentas, aumentando la eficacia de actuación al iniciarse dicho procedimiento en los primeros momentos.

- Otra característica común al fraude tradicional y al cometido a través de Internet – y que de nuevo, exige un mayor esfuerzo en la actuación de los CFSE – es el hecho de que la recepción de las denuncias se reciba de forma muy atomizada.

- Dada la complejidad y sofisticación técnica que rodea este tipo de fraude, se hace necesario disponer de medios técnicos avanzados que permitan realizar una investigación y tratamiento del caso apropiados.

- La especial naturaleza de Internet como medio utilizado para el desarrollo y explotación de nuevos tipos de fraude, hace patente la necesidad de definir protocolos avanzados de actuación en cuestiones que - como puede ser la validación de pruebas- repercuten directamente en el grado de éxito de la lucha contra actos delictivos de carácter fraudulento.

[58] Centro de Respuesta a Incidentes en Tecnologías de la Información para Pymes y Ciudadanos

Medidas de vigilancia y persecución de conductas delictivas

La magnitud de los delitos informáticos en los últimos años, junto a la complejidad técnica de la lucha contra éstos y la necesidad de coordinación con equipos internacionales han conducido a los cuerpos de seguridad de muchos de los países de la OCDE a crear grupos específicos dentro de ellos para la persecución de la ciberdelincuencia.

En España existen diversas unidades especiales integradas en los Cuerpos y Fuerzas de Seguridad del Estado que tratan de articular la lucha contra este tipo de prácticas criminales:

- La **Brigada de Investigación Tecnológica de la Policía Nacional** (www.policia.es/bit/cuer_bit.htm) es la unidad especializada dedicada a la persecución de los delincuentes, obtención y valoración de pruebas y puesta de ambos a disposición judicial. Para ello, es necesario disponer de una plantilla especializada y que reciba una formación constante.

  Esta Unidad trabaja también en colaboración con organismos públicos y empresas privadas para el logro de sus fines. Una de sus actuaciones de cooperación más importantes se desarrolla en el ámbito transnacional, colaborando con la policía de otros países en la investigación y detención de delincuentes.

  Su ámbito de actuación se extiende a todos los delitos informáticos, no sólo a los de contenido estrictamente económico, aunque éstos suelen ser la mayoría.

- El **Grupo de Delitos Telemáticos de la Guardia Civil** (www.gdt.guardiacivil.es) tiene como misión perseguir todos los delitos que se sirven de Internet o de las nuevas tecnologías para su comisión. Nace en 1996 con el nombre de Grupo de Delitos Informáticos. La evolución de los delitos telemáticos ha motivado diversas modificaciones en su estructura a lo largo de los años, hasta llegar a su actual composición.

  Dadas las crecientes necesidades de investigación en este ámbito, superiores a las disponibilidades de un grupo centralizado, se han creado los llamados EDITEs, Equipos de Investigación Tecnológica, para poder atender con mayor eficacia y eficiencia su trabajo. Este grupo ha participado y participa en muchos de los foros e iniciativas internacionales destinadas a la persecución del delito informático, colaborando con Europol e Interpol, el Grupo de Trabajo Latinoamericano sobre Delitos Tecnológicos (articulado en Interpol) o el foro internacional del G8 para el cibercrimen.

  La página web de este grupo presenta una recopilación de consejos a usuarios, a Pymes, a personas que realicen transacciones de comercio electrónico, a menores

y a padres para evitar algunos de los delitos más habituales. Asimismo, facilita un medio electrónico de denuncia a través de un simple enlace.

- Las **policías autonómicas**, como la Ertzaina (www.ertzaintza.net) y los Mossos d'Esquadra (www.policiadecatalunya.net/denuncies), tienen también especialistas en la persecución de los delitos informáticos.

- La **Agencia Española de Protección de Datos** (www.agpd.es), que tiene como objetivo contribuir al cumplimiento de la Ley Orgánica de Protección de Datos de Carácter Personal, la LOPD. Las tareas asignadas por esta ley son diversas, entre ellas algunas funciones de vigilancia de su cumplimiento, como hemos comentado, y de determinación de las sanciones que corresponden a su incumplimiento.

A nivel internacional se pueden encontrar las siguientes medidas de actuación:

- **Europol** (www.europol.europa.eu) organización europea creada en el marco de la Unión para la cooperación entre los cuerpos de seguridad de los países miembros, también tiene entre sus principios básicos de actuación la lucha contra la delincuencia informática, en la medida en que afecte a más de un Estado miembro o pueda ser considerada delincuencia organizada.

  Con este fin, Europol facilita el intercambio de información, a través de los llamados ELOs (European Liaison Officers), representantes en Europol de los cuerpos de seguridad de sus respectivos países; proporciona capacidad de análisis para apoyar las operaciones; genera informes estratégicos sobre el estado de la criminalidad; y proporciona conocimiento y soporte técnico a las investigaciones realizadas dentro de la UE.

- **Interpol** (www.interpol.int) ha creado cuatro grupos regionales especializados en delitos de contenido tecnológico, estando España integrada en el correspondiente a Europa. El European Working Party on Technology Crime, fundado en 1990 y se reúne tres veces anualmente [59]

  De cara al futuro, este grupo de trabajo se ha propuesto mantenerse a la vanguardia de la investigación sobre los delitos informáticos, incrementando su conocimiento y vigilancia de algunas de las tendencias más recientes al respecto: las redes de ordenadores zombis (*botnets*), la transmisión de voz a través de IP o determinados tipos de códigos maliciosos.

- El **G-8**, grupo integrado por los países más ricos del mundo, también ha desarrollado diferentes iniciativas destinadas a la lucha contra la delincuencia

[59] www.interpol.int/Public/TechnologyCrime/WorkingParties/default.asp

informática. En este terreno, se produce la creación del **Subgrupo sobre Delitos de Alta Tecnología**[60], nacido en 1997 bajo diez principios de actuación, entre los que se encuentran el desarrollo de leyes de amplia cobertura, que no ofrezcan resquicios a los delincuentes; la creación de protocolos de cooperación entre los participantes; la colaboración con la empresa privada; y la conexión y cooperación entre unidades operativas ágiles y disponibles en todo momento.

- Finalmente, aunque son muchos los cuerpos y fuerzas de seguridad de los diferentes países que luchan contra la ciberdelincuencia, es preciso destacar, tanto por la magnitud de sus actividades como por la profundidad de sus acciones al FBI, la Oficina Federal de Investigación estadounidense.

  Para perseguir los delitos informáticos el FBI (www.fbi.gov) ha creado, en cooperación con el National White Collar Crime Center[61], el **Information Crime Complain Center (IC3)**, organismo encargado de recoger y canalizar las denuncias acerca de delitos informáticos.

  Este centro realiza también una importante función de documentación, y es responsable de uno de los informes más conocidos sobre la tipología y evolución de los delitos informáticos, especialmente profundo en lo referente a los Estados Unidos.

  Con una finalidad divulgativa, intentando desdramatizar aunque no frivolizar el fraude online, el propio IC3 ha lanzado una página web llamada www.lookstoogoodtobetrue.com, en la que se describen diferentes tipos de estafas informáticas, dando consejos a los posibles objetivos para tratar de evitarlas.

4.4 Las Administraciones Públicas

La Administración no permanece ajena a este problema siendo el objetivo básico de cualquier administración garantizar el desarrollo social y económico de manera sostenible del territorio que se encuentre a su cargo. De este modo, los poderes públicos deberán reflexionar en torno a las posibles amenazas y frenos a este desarrollo, colaborando con los diferentes agentes sociales para su solución.

En este sentido, el compromiso de las autoridades con los sistemas de seguridad informática es claro y notable en los últimos años. Las actuaciones puestas en marcha abarcan todos los niveles y fases del proceso: desde la creación de diferentes métodos de prevención y disuasión, pasando por la participación en la reducción de los efectos, hasta

[60] El nombre original es G-8 Subgroup on High-Tech Crime.

[61] Organismo de carácter no lucrativo, creado a iniciativa del Congreso de los Estados Unidos.

la persecución de las conductas delictivas que afecten a la seguridad de los sistemas de información.

Medidas de carácter normativo

Son iniciativas destinadas principalmente a ejercer un efecto disuasorio entre los potenciales autores de este tipo de fraudes. A nivel europeo, la regulación normativa en materia de seguridad informática se puede encontrar en las siguientes normas:

- Directiva 95/46/CE del Parlamento Europeo y del Consejo, de 24 de octubre de 1995, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos.

- Directiva 97/66/CE del Parlamento Europeo y del Consejo, de 15 de diciembre de 1997, relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las telecomunicaciones. (Derogada por la Directiva 2002/58/CE).

- Directiva 2002/58/CE del Parlamento Europeo y del Consejo, de 12 de julio de 2002, relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las comunicaciones electrónicas. (Directiva sobre la privacidad y las comunicaciones electrónicas):

- Directiva 2006/24/CE del Parlamento Europeo y del Consejo de 15 de marzo de 2006 sobre la conservación de datos generados o tratados en relación con la prestación de servicios de comunicaciones electrónicas de acceso público o de redes públicas de comunicaciones y por la que se modifica la Directiva 2002/58/CE.

Las principales leyes que sustentan la protección de la seguridad informática en España son las siguientes:

- Constitución Española de 1978 en su artículo 18. 4 donde se establece que “La Ley limitará el uso de la informática para garantizar el honor y la intimidad personal y familiar de los ciudadanos y el pleno ejercicio de sus derechos”.

- Ley Orgánica 1/1982, de 5 de mayo, de Protección Civil del Derecho al Honor, a la Intimidad Personal y Familiar, y a la Propia Imagen.

- Ley 34/2002, de 11 de julio de Servicios de la Sociedad de la Información y Comercio Electrónico (LSSI-CE).

- Ley 32/2003, de 3 de noviembre, General de Telecomunicaciones.

- Ley Orgánica 5/1992, de 29 de octubre, de Regulación del Tratamiento Automatizado de los Datos de Carácter Personal. (LORTAD, vigente hasta el 14 de enero de 2000).

- Ley Orgánica 15/1999 de Protección de Datos, de 13 de diciembre (LOPD) y el Reglamento de Medidas de Seguridad (RMS).

- Código Penal, (CP), aprobado mediante Ley Orgánica 10/1995, de 23 de noviembre.

El entramado normativo se completa con otras normas con rango de ley que regulan aspectos relacionados con los soportes informáticos, muy especialmente la Ley de Propiedad Intelectual (Real Decreto Legislativo 1/1996, de 12 de abril), y por los correspondientes desarrollos reglamentarios surgidos a partir de estas normas.

En el ámbito europeo, la UE ha puesto en marcha diferentes iniciativas, dentro de la promoción general de la Sociedad de la Información, con un carácter mixto, tanto de divulgación y difusión, como de potenciación legislativa entre los países miembros.

De este modo, la Comisión Europea en el año 2000 no sólo instó al Consejo de la Unión Europea[62] a trabajar en una propuesta de armonización legislativa, sino que planteó la necesidad de establecer otro tipo de medidas no legislativas, así como favorecer la continuidad de las acciones destinadas a fomentar la seguridad en el ámbito de los diferentes programas europeos en marcha.

La Comisión determinó en 2004 la creación de ENISA, la **Agencia Europea de Seguridad de las Redes y de la Información** (www.enisa.europa.eu). Sus objetivos son:

- Asesorar a los estados miembros, así como a los propios organismos de la UE, en relación con cuestiones de seguridad de redes, y recopilar datos a este respecto.

- Fomentar la evaluación y los métodos de gestión de riesgos.

- Cooperar con el mundo empresarial y privado en busca de la expansión de buenas prácticas de seguridad.

- Respaldar el establecimiento de normas para el desarrollo de la Sociedad de la Información.

En mayo de 2006 la Comisión Europea plantea una estrategia basada en el diálogo, la asociación y la potenciación para afrontar algunos de los principales retos de seguridad

[62] Aunque los nombres sean muy parecidos, hay que recordar que el Consejo de Europa no tiene relación con la Unión Europea, salvo que muchos de sus miembros coinciden.

que se plantean, como el incremento de comunicaciones con dispositivos móviles, el aumento de los ataques y, especialmente relevante a este efecto, la sensibilización de la opinión pública.

Entre las iniciativas legislativas a nivel internacional destaca la **Convención del Consejo de Europa de Budapest (2001) acerca de cibercriminalidad**, con un triple objetivo: legal (delimitando el marco que se comentó con anterioridad); procesal (reforzando la acción de la ley y la justicia en la persecución de estos delitos); y cooperativo (tratando de poner en marcha iniciativas de cooperación entre los Estados firmantes).

Por lo que se refiere al Consejo de la UE, en el año 2005 planteó una decisión marco, que debe ser transpuesta a las legislaciones de los Estados miembros antes de marzo del año 2007, en la que se determina la tipificación legal de tres supuestos relacionados con los ataques a sistemas de información: el acceso ilícito, el perjuicio a su integridad y la intromisión ilegal en sus datos.

Es preciso señalar que la capacidad de este tipo de organismos es limitada, ya que, a diferencia del Consejo o de la Comisión de la UE, sus resoluciones no tienen fuerza legislativa directa en los países miembros. No obstante, las armas de la ONU en la lucha contra el delito se basan en su fuerza moral y la capacidad para promover acuerdos y convenciones amplios entre sus estados miembros.

En este sentido, la Organización ha desarrollado diferentes iniciativas destinadas a combatir el delito informático a escala global, en las cuales ha actuado de manera coordinada con otros grandes organismos supranacionales, como el G8, el Consejo de Europa o la Organización para la Cooperación y el Desarrollo Económico (OCDE). Así, la ONU ha convocado congresos, creado y financiado grupos de expertos y ha formado parte de los principales foros mundiales relativos al tema.

Finalmente, una de las líneas de trabajo de la OCDE gira en torno a la seguridad y privacidad informáticas: **Working Party on Information Security and Privacy** (WPISP)[63], Este organismo presenta informes sobre diferentes aspectos relativos a la seguridad informática, siendo uno de los más paradigmáticos el destinado a analizar las políticas de los Estados miembros relacionadas con el cambio de mentalidad hacia la seguridad informática.

Medidas de prevención y refuerzo de la e-confianza

Dentro de las medidas de prevención y confianza que la Administración ha puesto en marcha para asegurar y garantizar los Sistemas de Información y Comunicación en

[63] http://www.oecd.org/oecd/pages/home/displaygeneral/0,3380,EN-about-43-nodirectorate-no-no-no-13,FF.html

general, e Internet, en particular; el ***DNI electrónico***[64], se configura como uno de los programas más ambiciosos.

El DNIe, se posiciona no solo como una herramienta dinamizadora de la Sociedad de la Información, acercando a los ciudadanos el uso de la tecnología de una forma segura y permitiéndoles una interacción sencilla con dicha tecnología, es además una herramienta fundamental para la lucha contra las amenazas a las que se enfrenta la Sociedad de la Información: el fraude electrónico, la propagación del código malicioso, la suplantación de identidad o la ingeniería social,

El DNIe[65] permite establecer las bases para el desarrollo de tecnologías enfocadas a permitir las transacciones electrónicas seguras, posibilitando que el ciudadano pueda "identificarse" y verificar la identidad de su homónimo en la comunicación. Así mismo, posibilita la verificación y autenticación de la información enviada y recibida.

Amenazas tan peligrosas como el *phishing*, pueden ser sustancialmente erradicadas mediante el desarrollo de herramientas y conceptos basados en el DNIe como elemento de identificación y autenticación segura.

El DNIe debe de ser entendido no como una mera extensión del DNI actual, sino como una evolución hacia una herramienta que permite la interacción del ciudadano tanto en el mundo físico como en el mundo Internet.

Medidas relativas al estudio, formación y divulgación

Estas medidas están especialmente destinadas a ofrecer información a la opinión pública, así como proporcionar formación a ciudadanos y empresas sobre buenas prácticas y hábitos, así como mecanismos de prevención y defensa, para los usuarios finales utilicen y se beneficien de modo seguro y confiado de cualquier servicio o facilidad relacionado con las TIC, propia de la Sociedad de la Información de forma, y resulten menos vulnerables ante un posible delito de esta naturaleza.

En España, existen diferentes medidas de carácter divulgativo para mejorar el nivel de información y formación por parte de los usuarios.

Se pueden señalar en este sentido la labor desarrollada por el **Instituto Nacional de Tecnologías de la Comunicación** (INTECO), www.inteco.es, organismo promovido por el Ministerio de Industria, Turismo y Comercio. Una de las tareas que desempeña este

[64] http://www.dnielectronico.es/Asi_es_el_dni_electronico/

[65] La Ley 59/2003, de 19 de diciembre, de firma electrónica, ha venido a atribuir al Documento Nacional de Identidad nuevos efectos y utilidades, como son los de poder acreditar electrónicamente la identidad y demás datos personales del titular que en él consten, así como la identidad del firmante y la integridad de los documentos firmados con los dispositivos de firma electrónica, cuya incorporación al mismo se establece.http://www.dnielectronico.es/marco_legal/RD_1553_2005.html

organismo es adelantarse a las amenazas que para el desarrollo de la Sociedad del Conocimiento plantean los problemas de seguridad de los sistemas de información telemáticos. Por ello, INTECO viene participando en diversas iniciativas entre las que cabe señalar:

- El lanzamiento de Campañas específicas contra el Fraude Online y por la Seguridad en la Red (www.seguridadenlared.org). La seguridad y protección de los usuarios constituyen los objetivos principales de estas campañas ofreciéndose con esa finalidad servicios de formación e información al usuario de Internet, recursos y soluciones gratuitas de protección para el PC y un canal de denuncia entre los servicios más destacados.

- A través de la propia página web de INTECO, www.inteco.es se puede acceder a gran cantidad de contenidos y servicios sobre el estado actual de la seguridad de la información en España.

- Es destacable la elaboración de estudios y artículos, así como información estadística acerca del estado de las principales amenazas de seguridad y tendencias del fraude informático en España, como es el caso del presente estudio.

- Para combatir no sólo las actividades fraudulentas realizadas a través de Internet, sino para la lucha contra el código malicioso en general, INTECO ha puesto en marcha su **Centro de Respuesta a Incidencias en Tecnologías de la Información (INTECO-CERT para Pymes y Ciudadanos**), que difunde el estado de seguridad de las redes y las últimas alertas. La seguridad y protección de los usuarios de Internet constituye el objetivo principal del Centro ofreciéndose con esa finalidad servicios de formación e información, recursos y soluciones gratuitas de protección para los equipos informáticos y un canal de denuncia entre los servicios más destacados. Asimismo, INTECO ha creado el **Centro Demostrador de Seguridad para la PYME**, orientado a fomentar y difundir entre las pymes españolas el uso de las tecnologías de seguridad de la información y, por otra parte, para potenciar el sector de la seguridad de las TIC en España. Para ello, el Centro Demostrador se sitúa como un facilitador de mecanismos de demanda temprana, acercándose a las necesidades de la pyme a través de diversas líneas de trabajo.

- Iniciativas encaminadas a la detección y bloqueo de dominios .es fraudulentos, conforme a las directrices de un protocolo de actuación que será consensuado por todos los agentes del sector involucrados.

Dentro de esas propuestas se perfila, de un lado, la denominada *Red de Buzones Antifraude* a través de la cuál los diferentes actores implicados informarán de los fraudes online, haciendo acopio de la máxima información referida a los mismos.

De otro lado, se plantean actuaciones exclusivas de bloqueo para casos de *phishing* ocurridos con dominios .es

Asimismo, señalar el papel que desempeña la **Entidad Pública Empresarial Red.es**, www.red.es, adscrita al Ministerio de Industria, Turismo y Comercio y cuya función primordial es impulsar el desarrollo de la Sociedad de la Información resultando, de igual manera, bien conocida esta entidad, por la realización de actividades de divulgación, como por ejemplo, chaval.es.

4.5 Los usuarios y asociaciones de consumidores y usuarios

4.5.1 Medidas de actuación de los usuarios finales

Siendo en última instancia los agentes afectados por este tipo de conductas delictivas la actuación de los usuarios finales de los sistemas de información en Red a la hora prevenir y erradicar el fraude online es esencial.

Tratándose de un fenómeno basado en la ingeniería social (en el engaño), el usuario ha de asumir cierta responsabilidad en este tema, manteniendo un comportamiento prudente y seguro a la hora de usar dichos servicios. En el epígrafe 5.5 *"Recomendaciones dirigidas a los usuarios finales"* se abordará con mayor profundidad, cuáles son a juicio de los expertos, las conductas y actitudes adecuadas para utilización segura de la Red y la prevención del fraude online.

Desde el punto de vista técnico, no solo existen herramientas específicas para protegerse de este tipo de fraude, como los *firewall* o cortafuegos y las aplicaciones *anti-phishing*, que han de ser complementadas con el empleo de medidas de protección básicas – antivirus, anti-spam, anti-software espía – para lograr una navegación segura.

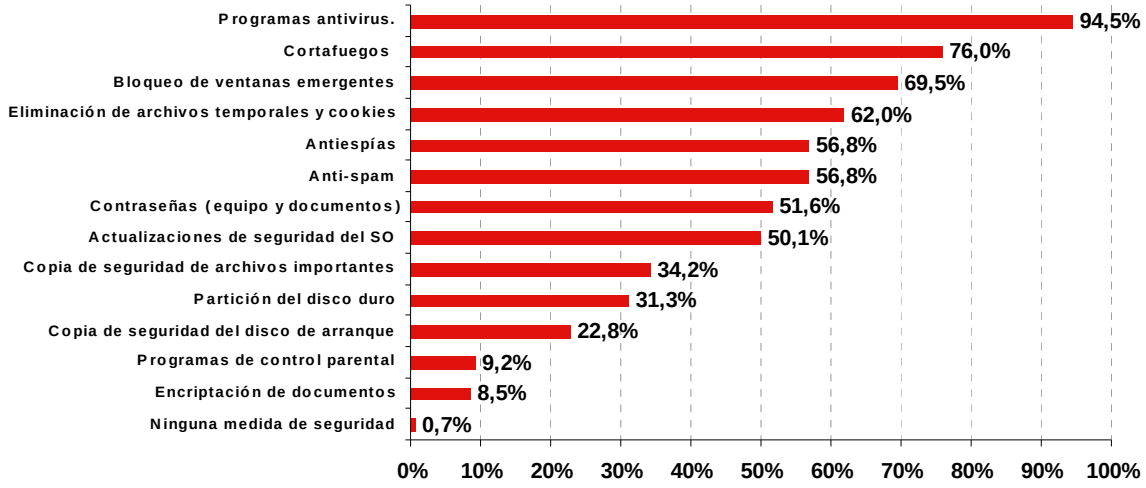
Por otro lado, con vistas a una protección global, la instalación de dichas soluciones informáticas ha de complementarse con la actualización de los sistemas operativos y programas. Es fundamental tener los equipos actualizados. Este hábito de seguridad puede ayudar a evitar la incidencia de los fraudes derivados de vulnerabilidades y fallos de seguridad de los sistemas y programas.

Siguiendo los datos del *Estudio sobre la Seguridad de la Información y eConfianza en los hogares españoles* elaborado por el Observatorio de la Seguridad de la Información de INTECO[66], y como se muestra en el Gráfico 45, la instalación de programas antivirus en los

[66] http://www.inteco.es/frontinteco/es/frontIntecoAction.do?action=viewCategory&id=6623&publicationID=50262

usuarios frecuentes de Internet en el hogar mayores de 15 años es prácticamente universal (94,5%). En segundo lugar, la medida de seguridad más utilizada son los programas cortafuegos (76%). En el tercer lugar del escalafón aparecen otras medidas de seguridad, como el bloqueo de ventanas emergentes (69,5%), la eliminación de archivos temporales y *cookies* (62%), los programas anti-correo basura y anti-espía (56,8% en ambos casos) y las actualizaciones de seguridad del sistema operativo (50,1%).

Gráfico 45: Porcentaje de utilización de medidas de seguridad en los hogares españoles en 2007



Fuente: INTECO

El referido estudio distingue dentro del listado total de medidas de seguridad, dos familias de medidas diferentes en atención al hecho de que la intervención del usuario tenga carácter pasivo o activo (medidas automatizables o no automatizables).

Por lo general, los usuarios se decantan por medidas de seguridad de carácter automatizable: son medidas que operan de forma automatizada en los equipos, esto es, no suelen requerir del usuario una atención específica. Son configurables determinadas acciones como, por ejemplo, conseguir la automatización de las actualizaciones de las medidas cada vez que el usuario se conecta a Internet. Esto facilita una gestión automatizada de las medidas que redunda en una mayor comodidad para el usuario y una mayor disponibilidad de tiempo. Además, todas las medidas pasivas contienen un sistema de seguimiento y monitorización de la situación de operatividad de la propia medida: estado de las actualizaciones, última actualización, configuración de descarga e instalación de actualizaciones, aplicación de avisos y estado.

4.5.2 Asociaciones de Consumidores y Usuarios

Las estafas a través de la Red, y en general, la existencia de elementos perniciosos para los navegantes, han motivado a los usuarios a organizarse para la defensa de sus derechos e intereses, generalmente a través de cauces asociativos.

En general, las asociaciones de usuarios se están especializando cada vez más en la lucha contra el fraude online dando una gran importancia a la información, formación y concienciación del usuario final en este tema. Así, desempeñan acciones de cara a proteger al usuario final de Internet entre las que destacan:

- Rastrear la Red para localizar páginas web fraudulentas.
- Realizar campañas de comunicación del *phishing*, tanto a nivel nacional como internacional, fundamentalmente vía Internet.
- Colaborar con los diferentes agentes implicados en la seguridad online.
- Disponer de un servicio de atención al cliente para ayudar a resolver dudas a los usuarios finales.

De esta forma, las asociaciones de usuarios y consumidores, ya sean específicas de Internet o de carácter general, españolas o extranjeras, han mostrado importantes niveles de preocupación por la seguridad de los sistemas de información, y han participado en la gestación de medidas de diferente índole, encaminadas a la promoción de la seguridad, la difusión y mejora del conocimiento de diversos aspectos relativos a ella, y la generación de cauces de información hacia la opinión pública para analizar los diferentes fraudes que se han producido a través de medios electrónicos.

En España, existen diversas asociaciones dedicadas a la defensa de los intereses del consumidor de servicios a través de Internet. Posiblemente las dos más conocidas son:

La **Asociación de Internautas (AI)**: Nace como entidad sin ánimo de lucro el 10 de octubre de 1998, partiendo de varias plataformas de usuarios de Internet que deseaban defender sus derechos respecto a las tarifas de telefonía.

Los fines establecidos en el artículo 4 de sus estatutos son “la defensa, información y educación de los usuarios y consumidores de las comunicaciones telefónicas y telemáticas, dado que éstas constituyen servicios de uso común, ordinario y generalizado”. De igual modo, se plantea la vigilancia de la actuación de los poderes públicos y la promoción de la tarifa plana.

La AI (www.internautas.org) viene realizando diversas actuaciones relacionadas con la seguridad en general, y con la prevención y detección del *phishing* en particular:

- Elaboración de un Informe anual sobre el *phishing* y otras amenazas en España, publicado en su página www.internautas.es

- Inclusión en su página web de un sistema de niveles de alerta de *phishing*, en función de los niveles de peligrosidad que se considere que existen.

- Incorporación en su sitio web de información específica sobre el *phishing*, incluyendo las últimas noticias que se han producido en torno al mismo.

- Articulación en su página web de un mecanismo de denuncia por correo electrónico.

La **Asociación de Usuarios de Internet (AUI)**. Es igualmente una entidad sin ánimo de lucro, nacida el 5 de julio de 1995, con ámbito nacional.

Sus fines fundamentales, según declara el artículo 2 de sus estatutos, son:

- "Promover, sin ánimo de lucro, el desarrollo de Internet, de la Sociedad de la Información y de las Nuevas Tecnologías así como del equipamiento, aplicaciones, servicios e infraestructuras necesarias para ello.

- Proteger y defender los intereses y los derechos de los Usuarios de Internet y de las Nuevas Tecnologías.

- Fomentar el buen uso de Internet, de las Nuevas Tecnologías y de sus aplicaciones en el hogar, en las empresas y en las Administraciones públicas; tanto para su uso en el ámbito personal como para su uso en actividades profesionales".

Está abierta tanto a personas físicas como jurídicas, por lo que cuenta con un buen número de asociados empresariales, entre los que figuran algunas de las empresas más importantes de nuestro país relacionadas con las tecnologías y sistemas de información.

Algunas de las acciones realizadas por la AUI (www.aui.es) en relación con el *phishing* y el fraude en Internet son las siguientes:

- Existencia de un espacio específico en su web relacionado con la seguridad de los sistemas de información, con consejos destinados a diferentes tipos de usuarios y vínculos a los principales organismos de denuncia.

- Documentos técnicos de divulgación disponibles en su web.

- Varias iniciativas destinadas a la promoción de la Sociedad de la Información.

Una de las entidades más activas a nivel internacional en la lucha contra el fraude en Internet es la **National Consumer League** estadounidense. Esta organización, no lucrativa y de carácter privado, ha desarrollado una importante cantidad de informes acerca de los diferentes tipos de fraude electrónico, con abundante información, descripción detallada de cada uno de ellos y consejos específicos para su prevención.

Con este fin, la asociación ha implantado dos programas, el Nacional Fraud Information Center, y el Internet Fraud Watch, destinados a la prevención del fraude en Internet utilizando principalmente la divulgación y proporcionando un canal ágil de contacto con las autoridades a la hora de denunciar casos de estafas electrónicas.

La asociación utiliza una página web exclusivamente con este fin. En www.fraud.org se proporciona información detallada sobre las estafas en Internet con una visión técnica y una cierta profundidad de análisis.

5 RESULTADOS CUALITATIVOS DE LA INVESTIGACIÓN: PROPUESTAS Y RECOMENDACIONES DE LOS PROPIOS AGENTES AFECTADOS POR EL *PHISHING*

Hasta el momento se han descrito las medidas genéricas y específicas que se vienen aplicando para la prevención y detección del *phishing* en los últimos años por parte de los distintos agentes afectados por este tipo de fraude o por otros de similar naturaleza.

En este capítulo del Estudio se recoge la percepción y opinión de expertos y usuarios con el fin de establecer un marco de análisis que aporte nuevas perspectivas y señale nuevas tendencias en las políticas y herramientas de seguridad

La consulta realizada para la recogida de información aporta, por sus características, una **nota diferenciadora** al conjunto del Estudio ya que se han considerado las opiniones directas de los propios afectados; así, el trabajo de campo ha consistido en:

- **3.076 encuestas a usuarios**: durante el mes de abril de 2007 se ha consultado vía online a usuarios de los servicios de información afectados por la práctica fraudulenta conocida como *phishing*.

- **40 entrevistas a expertos**, pertenecientes a los distintos sectores de actividad relacionados con la seguridad y el intercambio de información a través de la Red. Estas entrevistas se han desarrollado de forma presencial y en profundidad.

- **2 sesiones de grupos de debate**: la consulta efectuada durante la fase de investigación del Estudio se ha visto completada con la celebración de dos sesiones de debate de sendos grupos de trabajo integrados por expertos y conformados manteniendo una representatividad suficiente y común a los distintos perfiles consultados.

La fusión de las opiniones y valoraciones aportadas en las encuestas, entrevistas y grupos de debate, junto con la información obtenida en el análisis de la documentación nacional e internacional existente sobre la materia (publicaciones, legislación y documentos doctrinales y estadísticas), convierten este Estudio en una radiografía de la situación del fraude electrónico a través de Internet, en una útil herramienta de formación y divulgación, y en un referente de cara al diseño y seguimiento de las políticas públicas en esta materia.

5.1 Propuestas y recomendaciones dirigidas a las entidades financieras y otras empresas prestadoras de servicios a través de Internet

El usuario demanda de las entidades financieras y de las empresas de comercio electrónico que una pequeña parte de los beneficios que puedan obtener, por el ahorro en

costes que les supone prestar sus servicios en la Red, se reinvierta en información, concienciación y formación del usuario.

Así, se pone de manifiesto la necesidad de llevar a cabo las siguientes acciones divulgativas:

1. Ofrecer, bien individualmente por cada entidad o bien de forma conjunta, un servicio de atención telefónica y/o servicio online donde el usuario pueda realizar todo tipo de consultas relacionadas con Internet y su seguridad.

   Las opiniones recogidas orientan el contenido de dicho servicio en los siguientes términos:

   - Información preventiva: cómo protegerse para evitar ser víctima de un posible ataque de phishing.

   - Información reactiva: después de sufrir un ataque cómo se debe actuar.

2. Contar con un sitio web en el que se definan las pautas para realizar un buen uso de Internet. Promocionar la existencia de esa página en diferentes medios de comunicación (prensa, televisión, radio) para que de este modo puedan ser conocidas por todos los usuarios. Realizar un decálogo del buen uso de Internet, donde se establezcan una serie de normas y consejos a tener en cuenta por todos los usuarios que deseen trabajar a través de Internet de manera segura.

3. Una campaña de comunicación para la prevención del fraude, donde se informe a la población de las prácticas y hábitos de conducta seguros en Internet. En este sentido, y en referencia al *phishing*, se debe señalar como comportamiento básico y recomendable, no facilitar datos de carácter personal que se soliciten a través de un correo electrónico, aunque, aparentemente, provengan de entidades financieras. Asimismo, se reclama a dichas empresas la inversión en campañas formativas sobre las precauciones básicas que requiere el uso seguro de Internet dirigidas a perfiles muy concretos de usuarios (niños, jóvenes, adultos, tercera edad).

Por otro lado, se recogen como recomendaciones técnicas comunes a las entidades financieras y otras empresas prestadoras de servicios a través de Internet las siguientes:

1. Proteger sus servicios DNS[67], para que no puedan ser vulnerados ya que su manipulación puede ser crítica ante un ataque. Al igual que gracias a un número,

[67] El Domain Name System (DNS) es una base de datos distribuida y jerárquica que almacena información asociada a nombres de dominio en redes como Internet.

nombre y código postal localizamos un domicilio concreto dentro de una ciudad, Internet utiliza las llamadas direcciones IP (Internet Protocol) – que consisten en una serie numérica única – para llegar hasta una determinada página web. Pero como esa cadena numérica no resulta fácil de memorizar, se utilizan nombres de dominio que resultan mucho más fáciles de recordar y relacionan de manera más sencilla la web y el contenido al que se desea acceder. La relación entre dirección IP y el dominio se establece mediante el DNS (Domain Name System) correspondiente al que el navegador dirige sus consultas cada vez que el usuario solicita una página web, de forma que el proceso de resolución del nombre de dominio para averiguar la dirección IP a la que corresponde resulta en todo momento transparente al usuario.

Un ejemplo de fraude que se apoya en una modificación de estos registros es el *pharming* que, como se ha visto en capítulos anteriores, consiste en la manipulación de la respuesta a la consulta DNS que realiza el navegador, de forma que dirija al usuario a páginas diferentes a las originales y que han sido creadas al efecto para capturar información sensible de los usuarios, principalmente se corresponden con páginas de entidades de banca electrónica y de tiendas virtuales.

Por todo ello, el nivel de seguridad a aplicar sobre estos registros ha de ser muy tenido en cuenta a la hora de administrar sistemas de empresas que prestan sus servicios a través de Internet.

2. Utilizar herramientas especiales *anti-phishing* que adviertan al usuario ante cualquier sospecha sobre la autenticidad de la web a la que se accede. Estas herramientas se integran generalmente en la barra de herramientas del navegador y utilizan diferentes técnicas para localizar indicios de fraude. Uno de los métodos más efectivos para la identificación por parte de los usuarios de webs fraudulentas, además del análisis del dominio bajo el que se alojan, se basa en la actualización de las bases de datos sobre las que trabajan este tipo de herramientas por parte de diferentes agentes implicados en seguridad informática y que pueden denunciar la autenticidad de un determinado sitio. La implicación de los prestadores de servicios a través de Internet en estos intercambios de información puede también resultar útil para lograr la permanente actualización de este tipo de herramientas.

5.1.1 Propuestas y recomendaciones dirigidas a los bancos, cajas de ahorros y cooperativas de crédito

A continuación se exponen las recomendaciones específicas extraídas de las entrevistas y de las dinámicas de grupo dirigidas al sector financiero. Estas aportaciones se muestran agrupadas en dos grandes bloques o niveles:

Recomendaciones generales

1. **Aunar esfuerzos**: La lucha contra este fraude no será efectiva sin la colaboración internacional de empresas del sector de la seguridad informática, operadores de telecomunicaciones, las Fuerzas y Cuerpos de Seguridad y los Equipos de Respuesta a Emergencias Informáticas [68] gubernamentales (como el IRIS-CERT, el CCN-CERT o el INTECO-CERT)

   Usualmente los ciberdelincuentes atacan a diferentes entidades desde el mismo sitio y al mismo tiempo. Así pues, si la denuncia y el flujo de información se realizan individualmente desde cada entidad, la investigación se verá entorpecida. Por ello, es necesario que exista un sistema de cooperación operativa entre los FCSE y las entidades financieras para poder unificar las denuncias y las investigaciones, en función no de la entidad que es atacada, sino por el origen del ataque.

   Esta unificación en las denuncias, además va a permitir una lucha internacional más efectiva. Mientras que es poco probable conseguir una comisión rogatoria internacional tras un ataque aislado, sin embargo, agrupando esas denuncias será más fácil poner en funcionamiento a los cuerpos de seguridad a nivel internacional.

2. **Actuaciones globales**: El problema no se resuelve ni en el lado de la entidad financiera, ni en el lado del usuario de servicios de banca online, ni siquiera actuando sobre ambos; hay que actuar en un escenario mucho más amplio y tomar medidas orientadas a la consecución de diferentes tipos de objetivos.

   En este sentido, las posibles soluciones a este problema hacen necesaria la intervención de otros "actores" que no son ni las entidades financieras ni los usuarios. Se trata por tanto de impulsar la participación de aquellos agentes que –aunque en la actualidad no tengan demasiadas potestades en la materia – pudieran proporcionar mecanismos de prevención o reacción más efectivos, ya que, aunque sea de forma indirecta, se pueden ver implicadas en diferentes fases de un *phishing*. Por ejemplo, los proveedores de servicios de telecomunicaciones, cuyos equipos pueden alojar páginas web fraudulentas ante las que, una vez localizadas, se podrían implantar medidas preventivas de control sobre los accesos a las mismas. Por otro lado, los gestores de nombres de dominio como el ESNIC[69] a través de Red.es o la propia ICANN[70], pueden realizar tareas de vigilancia sobre nuevos dominios registrados que, debido por ejemplo a que presentan un parecido razonable con el dominio legítimo de alguna entidad bancaria, fuesen susceptibles

[68] CERTs: Computer Emergency Response Team – Equipos de Respuesta a Emergencias Informáticas) dependientes de los diferentes gobiernos de todo el mundo.

[69] Departamento de Red.es encargado del registro de nombres de dominio bajo ".es". Más información en www.nic.es

[70] Internet Corporation for Assigned Names and Numbers

de ser utilizados posteriormente para alguna práctica fraudulenta. Además, la actuación de organismos públicos competentes en seguridad como INTECO puede facilitar la localización de nuevos casos de *phishing* y la comunicación entre las entidades implicadas así como ofrecer información de referencia sobre el fraude electrónico en España.

Uso de mecanismos preventivos. Los usuarios deben poner todos los medios razonablemente a su alcance para evitar el posible fraude (herramientas anti*phishing* o antivirus actualizados, por ejemplo). Sus ordenadores domésticos deberían disponer de las herramientas y medidas de seguridad básicas para reducir el riesgo de infección.

Recomendaciones avanzadas

1. **Utilización de sistemas de Autenticación Fuerte o de "Autenticación de Dos Factores".** Se trata de medidas de seguridad recogidas actualmente por algunas legislaciones – como por ejemplo las recomendaciones realizadas al sector financiero norteamericano por parte del FFIEC, o las regulaciones seguidas en diferentes países de América o Asia. Es previsible la generalización de estos sistemas en los próximos años, bien como mecanismos de "autorregulación", o de "legislación" o bien "sistemas mixtos de autorregulación supervisada". Las entidades financieras deberían ofrecer, como regla general, la oportunidad a sus clientes de protegerse con sistemas de seguridad de autenticación fuerte. Se propone seguir manteniendo y consolidando las siguientes medidas:

    a. **Tarjeta de coordenadas.** Reducen el fraude, con resultados muy positivos. Aún aparecen casos en los que los usuarios son engañados y facilitan esta información, siendo posteriormente utilizada fraudulentamente; de ahí que resulte necesario combinar estos dichos sistemas de protección con una formación adecuada sobre su utilización.

    b. **Token de seguridad.** Dispositivo electrónico que permite la identificación del usuario, suponiendo una barrera muy efectiva que dificulta la comisión del fraude. A pesar de esta ventaja, este sistema de identificación de seguridad presenta algunos inconvenientes, como pueden ser: la incomodidad para el usuario, su elevado coste y la ralentización de las operaciones.

2. **Aplicación del modelo de negocio de las tarjetas de crédito**: El sistema de las tarjetas de crédito resulta, a priori, mucho más vulnerable tecnológicamente que los sistemas de banca por Internet. Sin embargo, en el negocio de las tarjetas de crédito se aplican desde hace años sistemas de prevención del fraude que resultan muy efectivos. Igualmente existen condiciones claras de limitación de la

responsabilidad para las partes implicadas en caso de estafa. Así, por ejemplo, los pagos con tarjetas de crédito o débito, emplean "mecanismos de intervención" que permiten localizar transacciones que presentan alguna característica extraordinaria y que por lo tanto pudiesen corresponderse con un caso de fraude.

De esta forma, los programas informáticos implantados en la gestión de cajeros automáticos cuentan con mecanismos de autodefensa que delatan cualquier movimiento de fondos extraño, ya sea por el lugar en el que se realiza la extracción, la frecuencia de las operaciones o la cuantía de las mismas. Estos mecanismos de intervención o autodefensa reducen los efectos de una posible manipulación de terminales así como el empleo de tarjetas de crédito clonadas[71] a través de la utilización de microcámaras camufladas[72] o lectores de bandas magnéticas.

En Internet – aún siendo un entorno mucho más complejo – existen mecanismos similares de prevención del fraude. Así, las tarjetas de crédito incorporan, cada vez más, tecnología de seguridad que reduce el riesgo de uso delictivo.

En esta línea, los expertos opinan que las entidades financieras deberían hacer un mayor esfuerzo inversor, si cabe, en sistemas de protección que han resultado ser muy prácticos y efectivos en las transacciones con medios de pago, de forma que contribuyan activamente a su popularización.

3. **Implementación de reglas lógicas y de comportamiento**. Estas reglas – ya utilizadas en la detección del fraude en el uso de tarjetas de crédito – y los llamados motores de comportamiento, se basan en la memorización de las pautas de conducta del usuario, permitiendo establecer alarmas de riesgo ante posibles casos de fraude. Es un sistema de protección que tiene un reducido coste, tanto económico como de funcionamiento, de la que el sector de las entidades de medios de pago cuenta con una sólida experiencia.

4. **Instauración de avisos a móviles mediante mensajes cortos (sms)**. Esta medida goza de la total aceptación de los expertos, puesto que permite la autenticación a través de dos canales diferentes y con una doble confirmación. Algunos entrevistados lo consideran la medida del futuro, puesto que es uno de los sistemas que mejores resultados está dando a nivel particular, especialmente en la operativa de algunas tarjetas de crédito.

[71] Noticia sobre un intento de fraude mediante el empleo de tarjetas de crédito clonadas.
http://noticias.ya.com/local/extremadura/14/03/2007/tarjetas-credito-cajero.html

[72] Noticia sobre un intento de fraude mediante el empleo de microcámaras camufladas.
http://belt.es/noticias/2003/03_enero/13_17/15/15_camaras_callejeros.htm

No obstante, sus puntos débiles son el alto coste que se produce al aplicarlos a cada transacción y la dependencia respecto de la cobertura de las redes inalámbricas dispuestas por el operador de telecomunicaciones. Además, en ocasiones, estos mensajes pueden tardar algún tiempo en llegar, lo que puede provocar ciertos problemas de agilidad en las transacciones.

Del mismo modo que las entidades de medios de pago ya han comenzado a instaurar dichos sistemas a través de acuerdos de cooperación con las entidades financieras, así como con el establecimiento de un marco regulatorio a nivel europeo, es imprescindible que se produzca la extensión de estos sistemas de protección al resto del sector bancario español.

En este sentido, merece especial reconocimiento la implantación que se viene produciendo de estos sistemas en el ámbito de las ***tarjetas de crédito EMV*** (Europay, Mastercard y Visa).

EMV es un estándar para la autentificación de pagos mediante tarjetas de crédito y débito que debe su nombre a las empresas que colaboraron en el desarrollo de dicho estándar (Europay, MasterCard, Visa). Una de las principales ventajas que supone utilizar sistemas de pago basados en el estándar EMV es el aumento de seguridad con la consiguiente reducción del fraude gracias al uso de algoritmos de cifrado.

Con la utilización de este estándar en las transacciones financieras se confirma la identidad del propietario de la tarjeta, solicitando el tecleo de un “Número de Identificación Personal” que sustituye, de este modo, la firma del recibo en papel. Con el tiempo, estos sistemas podrán utilizar otros medios de autentificación, como por ejemplo biométricos.

Se trata de una iniciativa europea que irá extendiendo al resto del mundo. Así, las tarjetas de crédito y débito incorporarán un certificado digital especial de seguridad, lo que por un lado obligará a las entidades financieras a cambiar todos los denominados TPV (Terminal Punto de Venta) y cajeros electrónicos, a cambio de lograr un nivel de protección tal, que asuman los reembolsos derivados de los casos de estafa que se pudieran producir. La implantación de estas tarjetas EMV comenzará a partir de 2008, y en el 2010 será obligatoria en todo el territorio de la Unión Europea.

Con estas medidas la entidad financiera ofrece un proceso operativo online menos vulnerable, lo que unido a unos hábitos de uso más seguros por parte de los usuarios, redundará en sistemas más protegidos y robustos.

Por otro lado, se recoge la recomendación de la necesidad de que los propios profesionales de las entidades financieras estén suficientemente informados sobre los sistemas de protección implantados por sus empresas y reciban, además, una formación básica en relación al fraude que existe en la Red, de modo que sean capaces de resolver

las dudas y preguntas de los usuarios cuando estos acuden personalmente a las oficinas o cuando plantean sus dudas a través de los teléfonos de atención al cliente.

5.1.2 Propuestas y recomendaciones dirigidas a las empresas prestadoras de servicios a través de Internet

Las empresas de compraventa de bienes y servicios a través de Internet (comercio electrónico), sitios web de subastas (como eBay o Mercadolibre), las organizaciones que permiten hacer donaciones a través de sus páginas web (por ejemplo, Cruz Roja, Greenpeace, o la Fundación Amigos del Museo del Prado) así como organismos públicos que dan servicios de e-Administración, como la Agencia Tributaria o la Seguridad Social, también han de ofrecer a sus clientes / usuarios las máximas garantías de seguridad cuando operan en la Red. Es por ello que, los expertos del sector consultados, proponen implantar las siguientes:

Recomendaciones generales

A continuación se enuncian una serie de aspectos genéricos que han de tener en cuenta las empresas en el diseño de sus sistemas, organizaciones y procesos, para con ello mejorar, no sólo la seguridad y la calidad de los servicios que prestan a sus clientes a través de Internet, sino también la confianza de éstos en dichos servicios[73]:

1. **Incidir en la seguridad como aspecto crítico para el negocio**. Si los activos intangibles son la parte más importante de cualquier negocio, la confianza, uno de los más importantes dentro de este grupo, es esencial en determinadas industrias que operan a través de la Red, como pueden ser la banca online o la distribución comercial.

2. Es importante **considerar los recursos destinados a proteger la seguridad de los sistemas de información como una inversión**, no como un gasto. Dado que la seguridad es un aspecto crítico para la organización, es necesario tratarlo como un fenómeno global, que trasciende todos los procedimientos, rutinas y actuaciones de la empresa.

3. **Es preciso conocer las debilidades, comportamientos y tendencias**. En este sentido, hay que realizar **estudios continuos y actualizados**, tratando de identificar las vulnerabilidades del sistema, lo que permitirá reaccionar ante ellas rápidamente, si es posible antes de que se materialicen.

4. Es imprescindible la **actualización de los programas y dispositivos de seguridad de la empresa**. Aunque esto no garantiza la plena seguridad del

[73] El Estudio sobre Seguridad en las Transacciones Electrónicas elaborado por la empresa S21sec ofrece recomendaciones interesantes en materia de seguridad, que pueden servir de corolario al conjunto de medidas anteriormente presentadas

sistema, sí se evitan algunas vulnerabilidades. Han de tenerse siempre las versiones actualizadas y los parches de seguridad de todos los programas utilizados, así como renovar y actualizar todo el software de seguridad de la empresa.

5. Es preciso **vigilar los accesos y el tráfico de información de los sistemas informáticos**. Hoy día los profesionales especializados pueden controlar permanentemente las entradas y salidas a los sistemas de información de una organización y todo el tráfico que se produce dentro de los mismos. Relacionando todos esos datos entre sí se pueden detectar intentos de acceso fraudulento o extracciones anómalas de información y comprobar si efectivamente se trata de un intento de delito, lo que permite, en caso de que así sea, tomar las medidas oportunas.

6. **Atención a los movimientos sospechosos que puedan producirse en el entorno**. Los servicios de vigilancia digital permiten detectar el registro de dominios o sitios web que intentan suplantar el nombre de la organización, copiar su web o utilizar fraudulentamente su marca. Atajar estos movimientos a tiempo puede evitar que la organización sea víctima de un futuro fraude o vea dañada seriamente su credibilidad.

7. Establecer una **política clara de acceso a la información**, que determine las personas, métodos, requerimientos y condiciones de distribución de diferentes tipos y niveles de datos. De esta forma, se podrá controlar mejor la seguridad de los activos digitales, lo que puede ser especialmente relevante en cuestiones como el mantenimiento de bases de datos de carácter personal o datos especialmente protegidos.

8. La disponibilidad de los instrumentos y políticas no sirve de nada si el personal de la empresa en su conjunto, no sólo los encargados de la seguridad informática, no saben **utilizarlos**. Por eso, es importante organizar un **plan de formación interna en materia de seguridad**. Todos los miembros de la organización, así como todo aquel que tenga acceso a los sistemas de información, deben recibir formación en materia de seguridad e implicarse en la tarea de mantenerla.

9. Finalmente, y como reflejo del valor estratégico que se ha conferido a la seguridad de los sistemas de información, hay que tratar de implantar una **cultura de la seguridad en la organización**, involucrando a todos sus miembros. Se trata de transmitir a los empleados y usuarios la importancia que la seguridad de los sistemas de información tienen para la empresa.

Recomendaciones avanzadas

Recomendaciones técnicas:

1. **La obligación de solicitar el código CVV2**. El código CVV2 (Card Verification Value) es un código de seguridad elaborado por las compañías de las tarjetas de crédito (Visa, MasterCard y American Express). Con este mecanismo de autenticación se identifica la posesión de la tarjeta empleada para el pago en las transacciones realizadas a través de la Red. Este código se debe introducir en el momento de la transacción económica por Internet para verificar que la tarjeta de crédito está en manos de su propietario, introduciendo un nivel de seguridad adicional a las transacciones realizadas. El formato de estos códigos es variable. Por ejemplo, los códigos CVV2 (Visa) y CVC2 (MasterCard) tienen 3 dígitos mientras que las tarjetas de crédito American Express tienen el código CID de 4 dígitos[74]

   A pesar de ser una medida de sencilla implantación, no todas las empresas online incorporan este mecanismo de seguridad a sus transacciones; por ello, sería necesaria su generalización.

2. **Sistemas inteligentes de prevención del fraude**. Consistiría por ejemplo en la introducción de un indicador que permita al usuario conocer, en función de los datos requeridos para una determinada operación, el nivel de riesgo que conllevaría su interceptación maliciosa antes de realizar dicha operación, advirtiéndole de la conveniencia de asegurarse que la realiza en un entorno seguro. De cara al prestador del servicio a través de la Red, un sistema inteligente de prevención del fraude puede basarse en la generación de avisos basados en resultados anormales en el proceso de validación de datos de una operación. Por ejemplo, sucesivos intentos de validación de datos sobre un mismo número de tarjeta de crédito variando su fecha de caducidad o el código CVV2 puede ser síntoma de un intento de uso fraudulento de dicha tarjeta y la operación podría quedar suspendida hasta comprobar que no se está haciendo un uso ilícito de la misma.

La implantación de estos sistemas de seguridad plantea algunos inconvenientes que pueden retrasar dicha implantación. Uno de estos inconvenientes es el tiempo empleado en el proceso, ya que supone un gran esfuerzo lograr activarlos, ponerlos en funcionamiento y que se lleven a cabo. Otro inconveniente es que se trata de medidas costosas económicamente para las entidades

[74] Más información en http://www.xonico.com.ar

Estas recomendaciones técnicas dirigidas a las empresas prestadoras de servicios a través de Internet se completan con las siguientes recomendaciones de carácter organizacional:

1. Establecimiento de un **Plan de Seguridad de la Información** son muchos los expertos que afirman que la primera medida que debería adoptar toda empresa que desee realizar un número elevado de transacciones a través de la Red, o que actualmente ya las realice, es una adecuada evaluación de los riesgos seguida de la elaboración de un plan de acción donde se concreten las medidas para reducir el riesgo de manera eficiente. Dicho plan ha de recoger las políticas de seguridad para controlar y minimizar los riesgos detectados y que han de ser seguidas por todos sus usuarios para lograr un aumento de la seguridad y de la calidad en el tratamiento de la información. La ISO 27001:2005 define el Sistema de Gestión de la Seguridad de la Información (SGSI) que, una vez implantado, asegura un nivel de seguridad adecuado y permite el acceso a la certificación correspondiente.

2. Establecimiento de **Políticas de Prevención.** Algunas de las medidas técnicas propuestas dejan muy pocos huecos para los estafadores, dificultando en extremo la realización de actividades fraudulentas a través de la Red. No obstante en otras, puede quedar espacio para el fraude; de modo que, en todo caso es esencial, para prevenir y combatir el *phishing*, la divulgación entre los usuarios de políticas de prevención, como las que se han enunciado anteriormente, evitando que estos resulten vulnerables ante las trampas de los ciberdelincuentes.

   En esta línea, la mayor parte de las instituciones financieras tienen en sus páginas de acceso algún tipo de advertencia, que indica a los usuarios que en ningún caso se les solicitará información personal o de acceso de sus cuentas mediante correo electrónico o medios similares.

3. Establecimiento de un **Plan de Formación** destinado a usuarios y a empleados. Por lo que se refiere a los primeros, se pueden realizar acciones de comunicación que establezcan claramente cuáles serán los canales de interacción entre los clientes y la empresa y aquellos canales que en ningún caso serán utilizados bajo ninguna circunstancia. En relación con los empleados, tienen que estar preparados para atender e informar convenientemente a los usuarios, tanto a nivel preventivo como de solución de incidencias de seguridad.

4. Establecimiento de un **Plan de Recuperación** para el caso en que se haya materializado la amenaza, es preciso que las empresas que fundamenten su negocio en transacciones electrónicas, dispongan de un plan de recuperación, que les permita retomar su actividad en condiciones adecuadas en el menor tiempo posible. Estos planes deben ser completos, incluyendo el análisis de elementos

físicos, lógicos, de comunicaciones, datos y personas, etc. Es imprescindible, además, que hayan sido probados antes de que sean necesarios ante una situación crítica.

5.2 Propuestas y recomendaciones dirigidas a los fabricantes y proveedores de servicios de seguridad informática

En relación a las recomendaciones que los expertos hacen a las empresas de seguridad, cabe mencionar:

1. **Que los productos que llegan a los usuarios cuenten con una certificación de seguridad**, con esquemas que obliguen a los fabricantes a contrastar dichos productos y verificar su calidad. Todo el software utilizado por los ciudadanos debe estar testado previamente en materia de seguridad por laboratorios independientes acreditados.

2. Se deben **desarrollar unos estándares de seguridad**, para poder validar y contrastar los certificados digitales por parte de laboratorios especialistas en protección de datos. De esta forma, se podría homogeneizar todas las certificaciones digitales que existen en el mercado, para establecer un protocolo de seguridad común. En este sentido, INTECO desarrolla en la actualidad los perfiles de protección para el eDNI en el ámbito de la Televisión Digital Terrestre (TDT), los dispositivos móviles y ordenadores de uso doméstico. Estos perfiles de protección serán los requisitos de seguridad mas adecuados para que los distintos desarrollos de fabricantes para estos ámbitos sean considerados por la industria y el ciudadano como seguros o de confianza. En definitiva, este proyecto dará pautas ciertas tanto a productores de tecnología como a los compradores de la misma.

3. **Mejorar las actuaciones por parte de los operadores para realizar un bloqueo de determinados servicios,** como puede ser el bloqueo del correo de salida que puede ser fácilmente monitorizable a través de un filtro que controle el tráfico del puerto 25, para aquellas máquinas cuya IP se identifique asociada a un uso malicioso del servicio de correo, distribuyendo *spam*, *malware* y troyanos, o un control en el acceso a aquellas máquinas que alojan sitios fraudulentos. Dado que la usurpación o mal uso de este tipo de recursos puede también producirse sin que su administrador sea consciente, la vigilancia y actuaciones por parte de los proveedores de servicios pueden resultar muy efectivas.

4. **Aplicación de políticas avanzadas de gestión de correo electrónico** proporcionando por ejemplo un servicio de salida de correo electrónico cortado por defecto, obligando a que el envío de ese correo se valide por el servidor del proveedor (ISP), donde se puede instaurar un mayor control del flujo de comunicaciones con restricciones y medidas de seguridad contra el mal uso del

correo electrónico y que, de esta forma, pueden resultar transparentes al usuario. Por otro lado, el usuario podría solicitar, a su voluntad el levantamiento de esta restricción, siempre y cuando, se le informe adecuadamente de las responsabilidades en las que incurre.

5.3 Propuestas y recomendaciones dirigidas al Poder Judicial y los Cuerpos y Fuerzas de Seguridad del Estado

Los expertos señalan las siguientes recomendaciones de cara a optimizar la operativa en la lucha contra el fraude a través de Internet del Sistema judicial y de los Cuerpos y Fuerzas de Seguridad del Estado.

1. Favorecer y estimular de forma activa la **formación continua** de jueces y fiscales sobre este tipo de delitos **a través de la Escuela Judicial y el Centro de Estudios Jurídicos**. Por otro lado es necesario **formar a jueces y fuerzas de seguridad en un lenguaje común**, de modo que permita un mayor grado de entendimiento entre las partes, y por lo tanto, una mayor efectividad en la lucha contra el fraude.

2. **Cooperación policial y coordinación entre los distintos FCSE**, **y además con los jueces y tribunales así como otros organismos de la Administración competentes en la materia**. En este sentido, es necesario el intercambio ágil de información, y aún más en todos los temas relacionados con Internet, donde la rapidez es primordial.

3. **Autoridad para requerir información relativa a las direcciones IP a los operadores de forma preventiva,** cuando se tengan sospechas fundadas de comportamientos ilícitos. Esto no significa que se obvie la obligación de solicitar un oficio judicial, sino que se pueda ir avanzando en la investigación debido a la volatilidad de las huellas electrónicas.

4. Para facilitar la persecución de este tipo de fraude, proponen que se instaure una **Fiscalía y juzgados especiales para la instrucción de delitos informáticos**, que disponga de los medios necesarios para dotar a estas unidades de la agilidad y rapidez necesaria en las comunicaciones.

5. **Existencia de comisiones rogatorias válidas en todo el territorio europeo** como instrumento indispensable para la eficacia de la justicia en el ámbito de la cooperación internacional.

5.4 Propuestas y recomendaciones dirigidas al Estado y las Administraciones Públicas

Antes de entrar a describir las propuestas y recomendaciones concretas dirigidas al Estado y las Administraciones Públicas conviene señalar que la Administración no sólo

desempeña un papel de tutelaje de los sistemas de información y comunicación a través de los distintos organismos públicos competentes (Jueces y Tribunales, FCSE, SETSI, AEPD, Red.es, INTECO, etc.) sino que además como entidad prestadora de servicios a través de Internet le son de aplicación las recomendaciones referidas en el punto 5.1.2. (Propuestas y recomendaciones dirigidas a las empresas prestadoras de servicios a través de Internet). Del mismo modo, y en calidad de usuario final de los servicios prestados a través de la Red – a través de su cuerpo de funcionarios, personal laboral y eventual de las Administraciones Públicas –, le son de aplicación las recomendaciones que se recogen en el punto 5.5 (Propuestas y recomendaciones dirigidas a los usuarios).

Las medidas propuestas a los poderes y administraciones públicas son necesariamente de carácter más genérico. Cada país tiene un marco regulatorio diferente, dentro del cual debe tratar de plantear medidas específicas que se ajusten a las recomendaciones generales destinadas a frenar el delito informático.

Los expertos opinan que sería de gran interés y relevancia, en la lucha contra el fraude en Internet, trabajar en relación a las siguientes líneas:

Desde el punto de vista normativo

1. **Instaurar una legislación en España que regule las transacciones comerciales y los flujos monetarios en la Red, exigiendo un sistema de autenticación fuerte.** Dicho sistema puede estar definido por diferentes elementos, según las diferentes opiniones de los expertos, pudiendo todo ellos coexistir y ser complementarios:

    - Sistemas generadores de claves de un solo uso (Token de seguridad)).
    - Tarjetas de coordenadas (consisten en una tarjeta física que tiene el usuario donde figuran una serie de letras y números, que se solicita al usuario para la realización de transacciones).
    - Certificados digitales en tarjeta.
    - DNI electrónico.

    Ese marco regulatorio generará en las entidades financieras la confianza suficiente para considerar los gastos necesarios como una inversión rentable en seguridad a medio y largo plazo y no como un gasto empresarial.

2. **Completar la LSSI-CE respecto a la obligación de conservar los datos por parte de los operadores.** En este punto, cabe señalar que la regulación sobre la Sociedad de la Información contenida en la LSSI-CE (Ley 34/2002) está siendo

objeto de modificación con el Proyecto de Ley de Medidas de Impulso de la Sociedad de la Información.

El anteproyecto elaborado por el Ministerio de Industria fue aprobado como Proyecto de Ley por el Consejo de Ministros y presentado ante el Congreso de los Diputados para su tramitación parlamentaria el 27/04/2007, calificado el 08/05/2007. En julio de 2007, el anteproyecto se encontraba en la Comisión de Industria, Turismo y Comercio del Congreso de los Diputados en el trámite del plazo para presentación de enmiendas, el cual fue ampliado hasta el 4 de septiembre de 2007.

Merece especial atención la disposición adicional tercera del Proyecto la cual dispone un: "Plan de mejora de los niveles de seguridad y confianza en Internet", tal que:

> *El Gobierno elaborará, en un plazo de seis meses, un Plan para la mejora de los niveles de seguridad y confianza en Internet, que incluirá medidas frente a códigos maliciosos, correos electrónicos no solicitados ("spam") y mensajes engañosos o fraudulentos ("phishing").*

3. La **normalización de la protección del software** haciendo obligatoria la implantación de medidas de seguridad en el software por parte de los fabricantes y proveedores.

4. A juicio de algunos expertos, debería reorientarse el enfoque normativo en cuanto a la **asunción de parte de la responsabilidad y el daño por el propio usuario víctima del fraude, cuando la utilización de la Red se haya hecho de forma no segura.** No obstante, dicha apreciación no es compartida por todos los agentes, especialmente por las asociaciones de usuarios.

5. **Armonización legislativa a nivel europeo en la tipificación de delitos y procedimientos jurídicos**. Resulta imprescindible, a juicio de los expertos, una coordinación en este sentido, cuanto menos, a nivel europeo para poder perseguir los fraudes de manera efectiva.

6. Se plantea la posibilidad de **introducir una asignatura en nuestro sistema educativo** sobre "buenos usos y procedimientos en la Red", puesto que Internet, se ha venido convirtiendo en una las herramientas fundamentales en el proceso de aprendizaje y en la obtención de información.

Desde el punto de vista ejecutivo y administrativo

Los diferentes perfiles de expertos consultados durante la investigación cualitativa llevada a cabo para la realización de este Estudio – entidades financieras, empresas prestadoras

de servicios a través de Internet, medios de pago, fabricantes y proveedores de soluciones de seguridad, Administración Públicas, Fuerzas y Cuerpos de Seguridad del Estado, abogados, juristas y expertos en derecho, y asociaciones de consumidores y usuarios – constatan la necesidad de trasladar a la Administración, de forma unánime, la demanda de una cobertura pública que garantice una adecuada seguridad de la información dentro del ámbito de las TIC. Esta necesidad de cobertura responde a la existencia, proliferación y profesionalización de amenazas y ataques de fraude online que ponen en riesgo la confianza de los usuarios de medios telemáticos en el uso de los mismos.

1. **Por parte de los expertos se propone la definición de un "superente" dentro de la Administración que aglutine las diferentes funciones en materia de seguridad.** Dicha propuesta consistiría en articular una única estructura organizacional en la que las diferentes funciones que actualmente la Administración desarrolla en materia de seguridad en los sistemas de información – gestión de dominios operatividad (Red.es), centro de alertas y respuesta a incidentes (INTECO), regulación y arbitraje (Comisión del Mercado de las Telecomunicaciones, CMT -www.cmt.es-) y capacidad normativa (SETSI - www.mityc.es/Telecomunicaciones-) y facultades para establecer medidas cautelares y persecución internacional – se desarrollen desde un único ente que asuma las funciones de dirección, seguimiento y coordinación de todas ellas. Un ejemplo de este tipo de organismo es el caso de FICORA[75] en Finlandia.

2. Además, se propone la **creación de un organismo encargado**, en coordinación con otros organismos homólogos fuera de nuestras fronteras, **de ponerse en contacto directo con los proveedores del país donde se detecte una amenaza, para poder bloquear una IP que está realizando una actuación ilícita.** Este aspecto redundará en investigaciones más ágiles y efectivas y la posibilidad de persecución de los delincuentes más allá de las fronteras de un país.

   Este organismo tendría que tener las facultades necesarias para poder evaluar la situación y establecer las medidas correctoras lo más rápidamente posible. Ante un ataque, tal como estamos viendo a lo largo del Informe, la velocidad de reacción es primordial.

[75] Finnish Communications Regulatory Authority. www.ficora.fi

En 1988 se funda el Telecommunications Administration Centre (TAC) dependiente del Ministerio de Transportes y Comunicaciones de Finlandia. A finales del año 2000 se toma la decisión de cambiar de nombre y en septiembre de 2001 se introduce el cambio de nombre por FICORA, convirtiéndose en la agencia que dependiente del Ministerio de Transportes y Comunicaciones de Finlandia continúa realizando la operación del TAC.

La misión de Ficora es proveer de conexiones de comunicación versátiles, efectivas y seguras a todo el mundo en Finlandia y promover el desarrollo de la Sociedad de la Información. Ficora está dividida en 7 áreas una de las cuales es Redes y Seguridad.

3. **Coordinación y participación de forma activa** de la Administración con el resto de los diferentes agentes implicados (entidades financieras, compañías de seguridad y otros prestatarios de servicios de Internet y la administración) en el proceso para prevenir el fraude online. Asimismo, se pide a la Administración que dinamice el trabajo realizado por los diferentes agentes, para que, de este modo, todos tengan un objetivo común y trabajen en la misma dirección, evitando la duplicidad y favoreciendo el enriqueciendo del trabajo y de los resultados obtenidos. En definitiva, siendo la Administración el elemento donde se asientan las bases de la seguridad online.

4. En este sentido, finalmente, se propone **activar un grupo, liderado y auspiciado por el sector público, que se dedique a I+D en el ámbito del fraude online.**

Desde el punto de vista formativo y divulgativo

A pesar de las medidas tecnológicas de protección que podamos establecer, la mayor parte de los fraudes de ingeniería social que se producen en la Red no se pueden evitar si falta la concienciación del ciudadano. Por ello, es tarea de los poderes públicos conseguir la concienciación de los usuarios – que son el punto más débil de la cadena de protección en y seguridad de Internet – para poder atajar el fraude online.

En cualquier caso, no basta con la **concienciación** sobre las prácticas fraudulentas, hay que abordar el tema desde una perspectiva más amplia de la seguridad en la Red. Como se ha expuesto, en el fenómeno del fraude se ha ido produciendo una transición, desde una mayor perspectiva de ingeniería social, hasta un desarrollo más tecnológico basado en el código malicioso con fines económicos ilícitos, donde no es imprescindible la participación consciente de la víctima para poder realizar la estafa. Por ello, es necesario que la información que se ofrezca al ciudadano contemple igualmente los temas relacionados con el *malware*, el equipamiento tecnológico para la protección de los equipos, etc.

Por ello, es necesario que desde la Administración se ofrezca una buena **formación** en relación a los adecuados usos y los abusos que se producen en la Red. Esta información, no tiene porque suponer alarma o desconfianza, simplemente precaución.

1. El impulso de **medidas de prevención destinadas a fomentar la concienciación de los usuarios en el buen uso de Internet** a través de una formación e información accesible y comprensible a todos los niveles de uso de la Red (básico, medio y avanzado) y para todos los perfiles (ciudadanos, empresas – particularmente pymes – y sector público).

2. **Dotar de formación continua al usuario en temas relacionados con la seguridad en Internet:** utilización de software legal, manejo de antivirus, prácticas

seguras en el comercio electrónico, etc. así como orientar dicha formación hacia un **protocolo de emergencia** que sirva como herramienta de información y asesoramiento **en el caso de ser víctima** por un caso de fraude online. Este protocolo deberá detallar los pasos pormenorizados de actuación.

3. Los expertos entrevistados consideran que un organismo público como INTECO debería ser uno de los **interlocutores principales con los medios de comunicación**, para que éstos tengan como **referencia una figura confiable y con criterio** a la que poder dirigirse a la hora de requerir cualquier tipo de información relativa al medio online y sus medidas de seguridad. En este sentido, es imprescindible que INTECO se incorpore en el discurso habitual de los usuarios cuando se trata la seguridad en Internet. **Los usuarios buscan un referente** que se dedique a impulsar la información, la formación, el estudio y la aplicación de nuevos mecanismos de seguridad.

   En relación a esta labor divulgativa, existe un problema añadido: la **falta de información veraz y datos rigurosos sobre el *phishing* y otras modalidades de fraude electrónico**. Existe una cierta inercia hacia la discreción, cuando no opacidad, a la hora de abordar el volumen de fraude que se está produciendo en España, y el nivel de seguridad real del que se dispone en las comunicaciones y transacciones a través de la Red.

   Por ello, desde la independencia y con los medios a su alcance que tienen los organismos públicos, y a través de la coordinación de diferentes entidades y organizaciones, es necesario que a través del **diagnóstico y la métrica** se facilite información veraz sobre la realidad en la que estamos inmersos, sin crear alarma social, y sin buscar culpables o víctimas, simplemente con la finalidad de construir indicadores que puedan orientar en que dirección debemos avanzar, y las medidas de prevención que podemos adoptar. El presente estudio es buena prueba de ello.

4. **Realización de un diagnóstico y medición y seguimiento de indicadores sobre el fraude online**. Para la realización de estos estudios tendría que existir una colaboración estrecha entre la administración y las entidades financieras y las Fuerzas de Seguridad del Estado – siempre manteniendo una absoluta confidencialidad de la información aportada por las entidades implicadas – que permitiría elaborar estadísticas e información cuantitativa para dimensionar el riesgo existente y así tomar las medidas oportunas de cara a la prevención.

5. Por otro lado, la Administración ha de ofrecerse como un **espacio imparcial en el que se pueden encontrar todos los expertos implicados** que abogan por la seguridad en Internet, convocando **foros, grupos de trabajo**, etc.

5.5 Propuestas y recomendaciones dirigidas a los usuarios y asociaciones de consumidores y usuarios

Las dinámicas de grupo realizadas durante la investigación de este Estudio han puesto de manifiesto que la proliferación del uso de Internet ha provocado que muchos usuarios se encuentren desinformados y actúen de manera intuitiva, o que busquen conocimientos a través de medios poco adecuados y de escasa fiabilidad. Así, los usuarios buscan información en páginas de Internet, en las que los contenidos no tienen por qué ser fidedignos o a través de experiencias personales de otros usuarios no especializados, sin conocer la similitud técnica del caso. Este modo de actuar provoca que los usuarios pongan en riesgo sus sistemas. Este hecho se ve agravado cuando el uso del ordenador es compartido, lo cuál ocurre en más del 60% de los hogares españoles[76]. De esta manera, es suficiente con que uno de los usuarios se encuentre desinformado y actúe de manera poco segura para que el resto también resulten perjudicados.

El usuario reconoce suplir esta falta de formación acudiendo a foros especializados, medios de comunicación convencionales e incluso a la experiencia de amigos y compañeros.

La principal conclusión de esta situación de desinformación, y la principal demanda de los usuarios, es la demanda por el usuario de una labor de tutelaje por parte de la Administración, que oriente en el desarrollo de las nuevas tecnologías, ofreciendo pautas para un buen uso de las mismas.

En general, todos los usuarios afirman que no existe la seguridad absoluta en Internet, y reconocen algunas situaciones de riesgo (la apertura de correos electrónicos y archivos adjuntos de fuentes desconocidas), considerando el *phishing* como “un fraude de toda la vida trasladado a Internet”.

Sin embargo, esa aparente sensación de inseguridad no impide que los usuarios continúen utilizando la Red a la hora de realizar transacciones económicas. Esto es debido a que los servicios y utilidades que brinda Internet se consideran irrenunciables al haberse integrado plenamente en su vida diaria, primando las ventajas derivadas del medio frente a las posibles desventajas.

Recomendaciones genéricas

Dentro de las recomendaciones genéricas para tratar de evitar los ataques en sus dos principales lugares de origen:

[76] 1ª oleada del Estudio sobre la Seguridad de la Información y la eConfianza en los hogares españoles. Observatorio de la seguridad de la Información de Inteco. 2007. www.inteco.es

1. En relación a la ingeniería social, una de las afirmaciones que más se suele hacer en todos los esquemas de recomendaciones a los usuarios es que "si es demasiado bueno para ser cierto, es que no es cierto". En este sentido, la mayor parte de los consejos van destinados a promover la utilización de la lógica por parte de los clientes.

2. Por lo que se refiere a las vulnerabilidades de los sistemas, la mayor parte de los impactos se producirán en el extremo más vulnerable del sistema, esto es, en el ordenador del cliente, ya que el ataque a los servidores de las empresas que proporcionan servicios en Internet requiere de más capacidad técnica.

Recomendaciones avanzadas

De otro lado, conscientes de la rapidez con que se producen los cambios y oportunidades dentro de las Tecnologías de la Información y la Comunicación y de que estas ventajas no dejarán de ser aprovechadas por los ciberdelincuentes, consideran necesario avanzar e ir incrementando el nivel básico de seguridad, con nuevas medidas tecnológicas que optimicen y garanticen en mayor medida su seguridad y complementen los hábitos y el comportamiento responsable y seguro del usuario.

Dentro de las recomendaciones avanzadas de carácter tecnológico se consideran:

1. El **DNI digital / electrónico** cuenta con una gran aceptación por parte de los participantes en las dinámicas de grupo y les ofrece máximas garantías.

2. El sistema de **tarjetas de coordenadas** también ofrece una elevada fiabilidad.

3. Las **tarjetas de crédito virtuales**, que modifican la clave en cada operación y se recargan con la cantidad necesaria, resultan también una medida muy útil.

4. El **teléfono móvil**, garantiza una segunda validación de las claves. Por lo que tener acceso a dos claves que proceden de canales diferentes obstaculizaría notablemente la labor del delincuente.

5. El uso de un **CD de arranque** para operaciones bancarias requiere de cierta preparación técnica y se percibe como un sistema de seguridad complejo.

6. El **sistema de claves** para la apertura de cada correo electrónico recibido resulta seguro, pero resulta demasiado incómodo y resta agilidad.

7. El **filtrado del correo electrónico**, de cierto contenido, por parte del operador está bien considerado, siempre que sea configurable por el usuario.

En todo caso, se debe procurar que la seguridad a nivel tecnológico, no se vuelva en contra del uso de Internet. Trabajar de forma más segura no puede suponer una pérdida de tiempo y un aumento de esfuerzo. El usuario no está dispuesto a perder la comodidad y rapidez que caracterizan a Internet.

Los usuarios difieren en la manera de tomar medidas y, sobre todo, a la hora de identificar los responsables de garantizar la seguridad en la Red. Si bien la mayoría de los usuarios opina que la Administración debería tomar parte, otros opinan que, además, los operadores de telecomunicaciones y las entidades financieras – e incluso algunos opinan que los propios usuarios – han de garantizar esa seguridad.

Como corolario a las recomendaciones indicadas se sugiere a los usuarios mantener las siguientes precauciones[77]:

1. **Si se recibe un mensaje que solicita información de carácter personal, no hay que responder, y ni siquiera hacer clic en él**. Las empresas no piden a sus clientes información a través de este tipo de medios. En caso de que exista alguna duda, esto es, de que se piense que la empresa puede estar requiriendo esta información, no hay que responder al mensaje, sino contactar con la empresa utilizando otra sesión del navegador (abrir una nueva ventana en nuestro navegador y teclear en ella la dirección web completa de la empresa), o bien por otro medio, y siempre ignorando el enlace insertado en el mensaje, que normalmente dirigirá al usuario hacia una trampa.

2. **Los prefijos pueden despistar**. No se debe confiar en los prefijos de los números de teléfono que aparecen en los mensajes dado que, al utilizarse protocolos de voz vía IP, estos pueden ser falsos o no estar situados en la zona en la que aparentemente debería. Por otro lado, se invita a los consumidores a ignorar estos números de teléfono, utilizando siempre los que las entidades han proporcionado a sus clientes a priori.

3. **Es importante utilizar programas de seguridad**. Su utilización es muy importante para evitar la instalación de códigos maliciosos en el ordenador de los usuarios finales.

4. **No conviene enviar información personal o financiera a través del correo electrónico**. Este medio de comunicación puede ser monitorizado por un tercero con vistas a ejecutar un fraude a través de herramientas de escaneo. Asimismo, se señala que la introducción de información personal o financiera a través de un formulario que lo requiera en una web debe hacerse en condiciones de seguridad,

[77] Conjuntos de recomendaciones confeccionadas a partir de las elaboradas por la Comisión Federal de Comercio estadounidense (FTC) en 2006 y las de la Nacional Consumer League

esto es, comprobando que hay un “candado” en la barra de estado del navegador o bien que la dirección comienza por https://, si bien estos indicadores han sido reproducidos por algunos de los estafadores más hábiles.

5. **Hay que comprobar los estados bancarios según se reciban**, para cotejar los movimientos y observar si existen algunos no autorizados. Si tardan en llegar más de unos días, conviene ponerse en contacto con la entidad financiera para comprobar si todo está correcto.

6. **Es importante tener precaución a la hora de descargar o abrir archivos adjuntos** de mensajes recibidos por correo electrónico, incluso si se conoce bien al remitente. Como ya se indicó anteriormente, este es uno de los métodos más habituales para tratar de instalar códigos maliciosos en los ordenadores de las víctimas.

7. **Conviene informar de los intentos de *spam* o de *phishing* que se reciban** a las autoridades competentes, así como a las entidades que están sufriendo el ataque, que suelen disponer de información en su página web sobre el medio de comunicación más adecuado.

8. **En el caso de sospechar que se ha sido víctima de *phishing*** conviene comunicarlo cuanto antes a las autoridades, para tratar de minimizar el daño que se pueda recibir, así como para intentar evitar el robo de identidad que suele acompañar al *phishing*.

9. **Conozca con quién está tratando**. Si contacta con algún desconocido, hágase con información sobre él a través de las administraciones públicas y entidades que la ofrecen. Conserve su dirección y teléfono (comprobando éste) por si hubiera algún tipo de problema a posteriori.

10. **Busque información sobre la resolución de conflictos**. Dado que los conflictos con compradores o vendedores de otros países pueden ser difíciles de resolver en caso de que surjan, busque de antemano la información de que suelen disponer las páginas de las empresas para conocer de antemano cómo se resuelven este tipo de problemas.

11. **El hecho de que no haya habido quejas no es ninguna garantía.** Las webs de los estafadores se abren y se cierran con mucha rapidez, de forma que normalmente no hay tiempo de que haya podido haber quejas de usuarios.

12. **No crea en promesas de dinero fácil**, negocios novedosos o una hipoteca gratuita o a un coste muy bajo, lo más probable es que sea una estafa.

13. **Entienda la oferta**. Un vendedor de buena fe le dará todos los detalles que requiera sobre el producto, el precio, la forma de pago, el modo de envío, las políticas de cancelación o reembolso y cualquier otro término o garantía.

14. **Resista a la presión.** Una auténtica organización no lucrativa que pide fondos le dará tiempo para que considere su opción, y no tratará de presionarle para que responda rápidamente, ni alegará que no admite un "no" por respuesta.

15. **Píenselo dos veces antes de participar en concursos organizados por empresas desconocidas**. Muchas veces los fraudes proceden de esta forma.

16. **Tenga cuidado con los suplantadores**. Alguien puede enviarle un correo hablando falsamente en nombre de una empresa u organización no lucrativa, o crear una página web casi idéntica a la de estas organizaciones. Si no está seguro de que está en contacto con la verdadera, utilice otro medio para realizar su transacción.

17. **Guarde su información personal**. No proporcione su cuenta bancaria o número de tarjeta de crédito a menos que esté realmente pagando por algún bien o servicio. El número de la seguridad social sólo será necesario en el caso de que esté pidiendo un crédito. Sea especialmente suspicaz si alguien que dice pertenecer a una empresa con la que usted trabaja le pide una información que la empresa ya tiene.

18. **Pague siempre por el medio más seguro**. Las tarjetas de crédito son el medio más seguro de pago online, dado que siempre se puede reclamar en el caso de que no se reciba el bien o servicio, o que éste no se ajuste a lo ofrecido. Las leyes suelen imponer límites a los daños al cliente si alguien hace un uso no autorizado de su tarjeta de crédito. Incluso estos daños son asumidos a veces por las empresas emisoras de tarjetas de crédito, según el acuerdo de utilización. Hay además algunas tecnologías que pueden añadir seguridad a las transacciones.

6 CONCLUSIONES

Los avances experimentados en muy pocas décadas en el marco de la Sociedad de la Información están dotando posiblemente a las personas de los mayores grados de desarrollo económico, social, cultural e individual que se han conocido hasta el momento. Los beneficios de las Tecnologías de la Información y la Comunicación son cuantiosos y considerables, tanto desde un plano individual como desde un punto de vista organizativo.

Del mismo modo que muchas aplicaciones, funcionalidades y servicios se han trasladado al mundo Internet, lamentablemente, el desarrollo de las tecnologías, y de Internet en particular, ha supuesto un nuevo entorno para la delincuencia, precisamente aprovechándose de las potencialidades que brinda este nuevo medio de comunicación. Así, se ha producido una **evolución tecnológica de las estafas tradicionales**, saltando a la Red bajo una nueva apariencia. Este es el caso del *phishing*.

Si bien, en las primeras fases las actividades delictivas suelen ser más rudimentarias y atentar contra bienes jurídicos más elementales, los grados más altos de progreso en las sociedades parecen una invitación a los delitos de naturaleza económica.

En este sentido, las Tecnologías de la Información y las Comunicaciones han supuesto una herramienta facilitadora de la realización de delitos a gran escala, con mayor eficiencia y, por lo general, mayor impunidad para el delincuente, dada la dificultad de perseguir este tipo de conductas ilícitas.

El *phishing* supone en parte una evolución tecnológica de algunas de las estafas tradicionales, aunque también significa en algunos casos la utilización de medios difíciles de detectar para un usuario poco informado para la comisión de un fraude. Dado que la Sociedad de la Información tiene bases globales, el crecimiento del *phishing* en España ha sido un reflejo de su evolución a escala mundial. Los datos nos muestran que, desafortunadamente, el *phishing* ha venido para quedarse.

El impacto de este delito es grave, tanto por las pérdidas que genera de forma directa a sus víctimas, como por generar desconfianza hacia las TIC e Internet, lo que supone un freno al desarrollo de la economía digital.

Dado que dichos efectos perniciosos del *phishing* afectan a todos: tanto particulares como empresas y administraciones públicas, las soluciones también deben partir del conjunto de la sociedad. De este modo, pueden y deben impulsarse diferentes **medidas de actuación contra el fraude en Internet** para tratar de erradicar o, al menos, paliar este problema.

Aunque muchas de las recomendaciones se repiten en las consultas realizadas a los diferentes agentes implicados en esta problemática – lo que viene a corroborar su importancia – se ha creído conveniente reflejar la particular visión de cada uno de ellos.

Individualmente, todos debemos ser conscientes de la magnitud de la amenaza sin caer en alarmismos, buscando niveles adecuados de formación e información sobre el problema que permitan poder evitar las formas más elementales de estafa. Por otra parte, somos responsables de utilizar las herramientas adecuadas para mantener nuestros sistemas de información con un grado de seguridad informática aceptable.

Las empresas, siguiendo las líneas de actuación marcadas por los expertos en la lucha contra el cibercrimen, deben mantener sistemas de seguridad apropiados a sus actividades. Por otra parte, la cooperación con otras empresas e instituciones es condición indispensable para la defensa frente al fraude. Además, deberían asumir el compromiso de formar e informar a los agentes con los que interactúan, especialmente trabajadores y clientes.

Los poderes públicos, además de promover todo tipo de iniciativas encaminadas a perseguir y erradicar este tipo de delitos, deben contribuir a la divulgación de todo conocimiento que favorezca ese objetivo. Esto implica, por tanto, no sólo el ejercicio de medidas legislativas, de policía o incluso pedagógicas, sino una constante actualización y valoración de la información existente, en colaboración con el resto de actores.

Como antes se mencionaba, el fraude ha existido siempre, e Internet sólo ha proporcionado un medio más a los delincuentes, quienes han aprovechado su globalidad, la escasez de legislación existente y la diversidad de desarrollo de ésta entre unos países y otros. Por ello, se hace imprescindible promover acuerdos y cooperaciones a nivel nacional e internacional. Mientras esto se perfecciona, se debe hacer hincapié en la prevención.

En primer lugar resulta imprescindible conseguir la **concienciación de los usuarios**, porque la cadena de protección tiene su punto débil en el último eslabón.

La seguridad en Internet es una cadena formada por operadores, proveedores de servicios, entidades financieras, medios de pago y usuarios. Una cadena es tan fuerte como lo sea su eslabón más vulnerable, que es en definitiva, el que se puede acabar rompiendo. A pesar de las medidas tecnológicas de protección que se puedan establecer, la mayor parte de los fraudes de ingeniería social que se producen en la Red no se pueden evitar si falta la concienciación del ciudadano.

Muchos usuarios todavía creen que toda la información que aparece en Internet es cierta y contrastada, se le supone la misma veracidad que tiene la prensa o la televisión. Lo mismo ocurre con los correos electrónicos que reciben. Es necesaria una buena formación en relación a los buenos usos y abusos que se producen en la Red. Esta información, no tiene porque suponer alarma o desconfianza, simplemente precaución.

Pero no basta con la concienciación, es necesaria, pero no suficiente. Se ha ido produciendo una transición en el fraude, desde una mayor perspectiva de ingeniería social, hasta un desarrollo más tecnológico, donde no es imprescindible la participación consciente de la víctima para poder realizar este fraude. Los nuevos dispositivos tecnológicos son capaces de perpetrar el fraude mediante el robo de información sensible, de manera que el sujeto sólo se da cuenta de lo que ha ocurrido, cuándo comprueba sus extractos del banco.

Paralelamente, ha de tenerse en cuenta la existencia de un problema añadido: la **falta de información y datos rigurosos** sobre el *phishing* y otras modalidades de fraude electrónico. Existe una cierta inercia hacia la discreción, cuando no opacidad, a la hora de abordar el volumen de fraude que se está produciendo en España, y el nivel de seguridad real del que se dispone en las comunicaciones y transacciones a través de la Red.

Sería muy deseable, que a través de la coordinación de diferentes entidades y organizaciones, se facilitase información veraz sobre la realidad en la que estamos inmersos, sin crear alarma social, y sin buscar culpables o víctimas, simplemente con la finalidad de construir indicadores que puedan orientar en que dirección se debe avanzar, y las medidas de prevención que se deben adoptar.

La concienciación y formación del usuario respecto a los usos y abusos de Internet debe ser una prioridad. Esta debe ser suministrada de un modo planificado, y dirigida a la sociedad en su conjunto, por lo que resulta necesario el apoyo público en todo caso. Hoy en día, hay numerosas fuentes donde obtener esta información, pero todos son pequeños esfuerzos individuales, que sólo abordan aquella parte que les puede afectar particularmente, según el tipo de agente del que se trate.

Resulta sorprendente que los usuarios residenciales tienen una menor percepción del riesgo que los propios expertos. Esto podría explicarse por un desconocimiento de la realidad en la que viven inmersos. A pesar de que muchos son conscientes de los fraudes que existen en Internet no parecen tomar las medidas de seguridad imprescindibles para poder desenvolverse dentro de la Red con garantías, por falta de formación, de concienciación o simplemente porque lo asumen con resignación.

En relación al *phishing* no existe un consenso generalizado cuando se aborda el tema de su **posible evolución**. Mientras que una parte considera que este fenómeno fraudulento, y sus efectos, han alcanzado los máximos niveles de actuación y perjuicio; para otra parte, especialmente entre las asociaciones de usuarios, se considera que todavía no se han alcanzado esos niveles máximos de riesgo, recomendando, en consecuencia, la adopción de hábitos y comportamientos seguros y responsables tanto en la navegación a través de la Red como en la utilización de otros medios telemáticos.

Algunos expertos, tanto en el sector financiero, como en otros sectores creen que se debe de ampliar el concepto de *phishing* hacia un concepto más global de fraude online. Existen nuevas técnicas que en realidad son variaciones del *phishing* tradicional. Recientemente, han aparecido casos de *phishing* tradicional en diferentes países, pero en un nuevo escenario: la telefonía IP y la telefonía móvil (*vishing*), junto con la recepción de sms (*smishing*).

Otro factor fundamental, es la **profesionalización del fraude**, desde la delincuencia cotidiana, hasta las mafias, y el crimen organizado dentro de la Red. Esta organización ha permitido una mayor sofisticación, y desarrollo tecnológico en los mecanismos de fraude a través de una coordinación, e intercambio de información entre los malhechores.

La introducción de nuevas medidas tecnológicas ha producido como resultado que el fraude se desplace de un sitio a otro. Un ejemplo claro es el fenómeno del *phishing*. Se ha comprobado que el fraude se mueve de una entidad a otra, dependiendo de la vulnerabilidad de las medidas de seguridad instauradas.

Para intentar paliar el problema de seguridad, es imprescindible la **coordinación entre todos los agentes implicados**. Ninguna solución es válida, si sólo se aborda desde un único ámbito, ya sea desde un punto de vista social, tecnológico o legal. La lucha contra el fraude en la Red, tiene que ser una prioridad de todos los intervinientes: usuario residencial, empresas y administración.

A pesar de este objetivo común, no es tarea fácil establecer acuerdos, y políticas consensuadas de actuación, ya que están presentes intereses, principalmente económicos e incluso políticos, que existen en Internet. Estos intereses, normalmente contrapuestos, entorpecen los esfuerzos de mejora de cara a solventar el problema.

Desde los diferentes agentes se reclama la presencia de una entidad pública que coordine las diferentes medidas, que cada uno parece estar adoptando por su cuenta y riesgo. Es necesario establecer un marco en el que se definan unas mínimas reglas de juego, en las que los participantes conozcan sus derechos y obligaciones.

Por otro lado, las medidas no se pueden establecer unilateralmente, es imprescindible una cooperación y un compromiso, al menos a nivel europeo. Esto incluye, en todo caso, la armonización de la legislación, tipificación, intercambio de información, procedimiento judicial, y actuación policial.

Por ello, finalmente, desde los diferentes agentes se reclama la presencia de una figura que dinamice todo el proceso de mejora de la seguridad en Internet: es necesario que este ente reúna, en un espacio imparcial, a todos los agentes y se aúnen esfuerzos en la misma dirección tanto preventivos como reactivos. Así, se considera que ese ha de ser la Administración, quien cumpla esa **labor de tutelaje y coordinación.**

En este sentido, el Instituto Nacional de Tecnologías de la Comunicación a través de sus tareas de diagnóstico, divulgación y asesoramiento – de la mano del Observatorio de la Seguridad de la Información – así como la prestación de servicios y la puesta en marcha de diferentes proyectos destinados a ciudadanos, empresas y administraciones en el campo de la seguridad tecnológica y de la información – como el Centro de respuesta a Incidentes en Tecnologías de la Información para Pymes y Ciudadanos[78] (INTECO-CERT) o el Centro Demostrador de Seguridad para Pymes – ha ido posicionándose como referente, nacional e internacional, en el ámbito de las Tecnologías de la Información y la Comunicación, en general, y de la Seguridad en Internet, en particular.

Así pues, por parte de los propios afectados (entidades financieras, fabricantes, usuarios, etc.) se percibe, de manera necesaria, una colaboración exhaustiva y continuada de INTECO con el resto de agentes interesados en informar, formar, dinamizar y potenciar la seguridad de la información a través de la Red, considerándose el momento actual, como momento oportuno de avance en esta línea de trabajo.

[78] En este último caso, heredero del Centro de Alerta Temprana sobre Virus y Seguridad Informática (CATA)

7 REFERENCIAS BIBLIOGRÁFICAS

Administración pública

- Agencia Española de Protección de Datos. Guía para la lucha contra el *spam*. http://www.uv.es/siuv/cat/norm/luchas*pam*.pdf

- Dirección Nacional de Protección de Datos personales. Ministerio de Justicia y Derechos Humanos. Argentina. Recomendaciones de la Dirección Nacional de Protección de Datos Personales. http://www.jus.gov.ar/dnpdpnew/recomendaciones/Recomendaciones_Internet.pdf

- FDIC (Federal Deposit Insurance Corporation) . (2004). The Use of Technology to Mitigate Account-Hijacking Identity Theft. 12/10/2004. http://www.fdic.gov/consumers/consumer/idtheftstudy/technology.html

- Federal Financial Institutions Examination Council. (2006). IT Examination Handbook. http://www.ffiec.gov

- Federal Trade Commission Bureau of Consumer Protection Office of Consumer and Business Education. (2003, 2004, 2005). National and State Trends in Fraud & Identity Theft (2003, 2004, 2005). http://www.consumer.gov

- Federal Trade Commission Bureau of Consumer Protection Office of Consumer and Business Education. (2005). Alerta de la FTC para Consumidores: Cómo Evitar que lo 'Pesquen' con una Red de Estafa Electrónica. Junio, 2005. http://www.ftc.gov/bcp/conline/spanish/alerts/s-*phishing*alrt.pdf

- Instituto de Ingeniería del Conocimiento. UAM. Lynx: Sistemas de detección de fraude de medios de pago. Proyecto cofinanciado por el Ministerio de Industria, Turismo y Comercio, dentro del Plan Nacional de Investigación Científica, Desarrollo e Innovación Tecnológica 2004-2007. http://www.iic.uam.es/flash/Lynx.swf

- Instituto Nacional de Estadística e Informática (INEI) de Perú. (2000). Amenazas en Internet. Marzo, 2000. Lima. http://www.pcm.gob.pe/PORTAL_ONGEI/seguridad2_archivos/Lib5121/Libro.pdf

- INTECO. (2006). Análisis mensual del Indicador de Peligrosidad del Correo Electrónico (IPCE) – Varios informes. http://inteco.red.es/observatorio/estudios.html

- La delincuencia informática sólo se puede combatir con una política internacional de Conservación de Datos. 2ª Jornada del Congreso Europeo de Protección de Datos.

30/03/2006. Madrid. https://www.agpd.es/upload/Prensa/Nota%20%20Jornada2%20ma%F1ana_3_4_06.pdf

- López Bernal, P.P. (2006). Servicios antifraude desde la cooperación interbancaria. Representante Grupo Seguridad- CCI. 24/01/2006. http://www.socinfo.info/seminarios/pasarelas/CCI.pdf

- OCDE. (2005). Scoping study for the measurement of trust in the online environment.

- Oficina nacional de tecnologías de información (onti). (2006). Recomendaciones para evitar ser victima del "*phishing*". Coordinación de emergencias en redes teleinformáticas de Argentina. Version 1.0. Agosto, 2006. http://www.arcert.gov.ar/webs/tips/recomendaciones_*phishing*.pdf

- Red.es y AECEM - FECEMD. (2006). Estudio sobre Comercio Electrónico B2C 2006. http://inteco.red.es/observatorio/estudios.html

- Red.es. (2005). Estudio sobre Comercio Electrónico B2C 2005. http://inteco.red.es/observatorio/estudios.html

- Red.es. (2006). Desarrollo y avance de la Sociedad de la Información en el ámbito empresarial. http://inteco.red.es/observatorio/estudios.html

- Red.es. (2006). Magnitudes Sociodemográficas de Internet. http://inteco.red.es/observatorio/estudios.html

- Romero, C.A. (2001). Comisión multisectorial encargada de elaborar y proponer las acciones necesarias para la implementación de las medidas recomendadas en la resolución Unga 55/63, destinadas a la lucha contra el uso criminal de las tecnologías de la información: Estado Situacional de las Actividades Realizadas. Ministerio de Transportes y Comunicaciones. Mayo, 2001. http://www.alfa-redi.org/documentos/i-taller-delitos-informaticos/Taller_INTERPOL.ppt

- Undécimo Congreso de las Naciones Unidas sobre Prevención del Delito y Justicia Penal. 18-25/04/2005. Bangkok (Tailandia). http://www.unis.unvienna.org/pdf/05-81509_S_1_SFS.pdf

- UOC- Red.es. (2005). Jornada Riesgos Penales de la banca online: Sistemas de prevención del fraude online. 16/12/2005. http://www.red.es/prensa/notas/diciembre_05/cata_uoc.pps

Ámbito judicial y jurídico

- De Sousa Mendes, P. La responsabilidad penal de las personas jurídicas en el ámbito de la criminalidad informática en Portugal. Fundación de Ciencia y Tecnología. Lisboa. http://www.hacienda.go.cr/centro/datos/Articulo/La%20Responsabilidad%20penal%20de%20las%20personas%20jur%C3%ADdicas%20en%20el%20%C3%A1mbito%20de%20criminalidad%20en%20Portugal.doc

- García Noguera, N. (2005). *Phishing*: Un peligro para la banca online. Abogados Portaley Nuevas Tecnologías S.L. 04/04/2005. http://www.delitosinformaticos.com/propiedadintelectual/*phishing*.shtml

- Libano Manzur, C. (2000). Los Delitos de *Hacking* en sus Diversas Manifestaciones. AR: Revista de Derecho Informático. Edita: Alfa-Redi. ISSN 1681-5726. Abril, 2000. http://www.alfa-redi.org/rdi-articulo.shtml?x=453

- Pérez, C.; Zorraquino, A.; Xavier Ribas, X. (2005). Internet, 10 años después: Retos jurídicos y de negocio. Landwell - PwC, "La Caixa" y la Fundación Barcelona Digital. 14/12/2005. Barcelona. http://www.bcndigital.org/debats/pdf/Resum141205_cast.pdf

- Read, P.; Bencosme, A. (2001). Los delitos informaticos. XV Congreso Coladic: Soluciones Concretas a Problemas Contemporáneos. http://www.coladicrd.org/biblioteca01.php

- Sánchez Magro, A. El ciberdelito y sus implicaciones procesales. En “Principios de Derecho en Internet” (Dir: Pablo García Mexía). http://www.tirantonline.com

- Tinajeros Arce, E.P. Criminalidad informática en Bolivia. Informática Jurídica. http://www.criptored.upm.es/guiateoria/gt_m001a.htm

Asociaciones

- American Online y National Cyber Security Alliance. (2005). AOL/NCSA Online Safety Study. http://www.staysafeonline.org/pdf/safety_study_v04.pdf

- Anti-Phishing Working Group. (2004, 2005, 2006). *Phishing* Activity Trends (varios informes). http://www.anti-*phishing*.org

- Anti-Phishing Working Group. (2003). What is *Phishing* and *Pharming*?. Diciembre, 2003. http://www.anti-*phishing*.org/solutions.html

- Asociación de Usuarios de Internet . (2006). Delitos informáticos. 01/12/2006. http://actua.aui.es

- Financial Services Technology Consortium. Understanding and Countering the *Phishing* Threat. A Financial Services Industry Perspective. (2005).

- Luque Guerrero, J.M. (2005). Muleros las otras victimas del *phishing*. Comisión de seguridad en la Red. Asociación de Internautas. http://seguridad.internautas.org/html/1/511.html

- National Consumer League. (2006). A Call for Action. Report from the National Consumers League Anti-*Phishing* Retreat.

- Pérez Nuevo, B. (2006). La AUI elabora una lista con los fraudes más comunes de la Red. Asociación de Usuarios de Internet. 21/06/2006. Madrid. http://www.copianos.com/es/content/download/1117/5537/version/1/file/La_AUI_elabora_un_ranking.pdf

Estudios académicos

- Conceptualización y generalidades del fraude informático. http://www.monografias.com/trabajos12/conygen/conygen.shtml

- Andrés López, O.; León Santibáñez, N. (2005). Monografía teórica e Investigación de virus y antivirus. Ingeniería de sistemas y computación. Universidad Tecnológica de Pereira (Colombia). http://gpsis.utp.edu.co/omartrejos/descargas/Monografia%20Virus%20y%20Antivirus.pdf

- Ballestero, M.P. (2003). El fraude en Internet, freno en la expansión de las tecnologías de redes. CEPREDE, Centro de Predicción Económica. Facultad de CC.EE y EE.- UAM. 21/03/2003. http://www.n-economia.com/informes_documentos/ALERTA_NE_02-2003.PDF

- Dhamija, R.; Tygar, J.D.; Hearst, M. (2006). Why *Phishing* Works. 22-27/04/2006. Montréal, Québec, Canada. http://people.deas.harvard.edu/~rachna/papers/why_*phishing*_works.pdf

- Drake, C.E.; Oliver, J.J.; Koontz, E.J. (2005). Anatomy of a *Phishing* Email. Working Paper.

- Escuela universitaria de informática (Universidad politécnica de Madrid). (2006). Libro Electrónico de Seguridad Informática y Criptografía. Escuela universitaria politécnica (Universidad de Lleida). Versión 4.1. http://www.criptored.upm.es/guiateoria/gt_m001a.htm

- Fernández de Soto, M.C. (2001). Atipicidad relativa en los delitos de falsedad, hurto, estafa y daños informáticos. Escuela de Derecho - Santa Marta. Universidad Sergio Arboleda. http://www.usergioarboleda.edu.co/biblioteca/documentos/der.018.htm

- Jagatic, T.; Johnson, N.; Jakobsson, M.; Menczer, F. (2005). Social *Phishing*. Indiana University. Working Paper.

- Landavendre Contreras, M.L.; Soto Campos, J.G.; Torres Lipes, J.M. (2000). Delitos Informáticos. Universidad de El Salvador. http://www.e-libro.net/E-libro-viejo/gratis/delitoinf.pdf

- Lozano Gutiérrez, M.C.; Fuentes Martín, F. Las respuestas emocionales del visitante de un sitio web de banca online. Universidad Politécnica de Cartagena. http://www.oei.es/salactsi/banca.PDF

- Manson, M. Legislación sobre delitos informáticos. http://www.monografias.com/trabajos/legisdelinf/legisdelinf.shtml

- Martín, I.G. Fraude en la Banca Online: un riesgo a tener en cuenta. CEPREDE, Centro de Predicción Económica. Facultad de CC.EE y EE.- UAM. http://www.n-economia.com/informes_documentos/ALERTA_NE_16-2005.PDF

- Meroño Cendal, A.; Soto Acosta, P. (2006). ¿Se cumple la legislación sobre sociedad de la información? Situación de empresas murcianas. Universia Bussiness Review, actualidad económica. Grupo Recoletos Comunicación. primer trimestre, numero 009. Madrid. http://www.universia.es/ubr/pdfs/UBR0012006088.pdf

- Ruiz, L.R. (2006). Uso ilícito y falsificación de tarjetas bancarias. Revista de Internet, Derecho y Política. UOC. http://www.uoc.edu/idp/3/dt/esp/ruiz.pdf

- Tenzer, S.M. (2004). Riesgo Informático: Nueva modalidad a través de Internet: "*Phishing*". Instituto de Computación de la Facultad de Ingeniería, materia "Procesamiento de datos II" (Ingeniería de Software). Universidad de la República de Uruguay. http://www.ccee.edu.uy/ensenian/catcomp/material/*phishing*.PDF

Legislación

- Delitos informáticos. http://derecho.eui.upm.es/DELITOS.doc

- Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico. http://www.boe.es/boe/dias/2002/07/12/pdfs/A25388-25403.pdf

- Ley de Comercio Electrónico. Noruega. (2003). http://www.uaipit.com/files/documentos/pdf/0000004740_Electronic%20Commerce%20Act.pdf

- Ley que Castiga el Uso de Identidad Fraudulenta en lnea. (2004). EE.UU http://www.uaipit.com/files/documentos/pdf/0000005531_Fraudulent%20On-line%20Identity%20Sanctions%20Act.pdf.

- (2005). Reglamento sobre la Protección del Consumidor en Ventas a Distancia. 11/03/2005. Reino Unido. http://www.uaipit.com/multilingue/documentos.jsp?len=es

- (2003). Ley contra el *Spam*. 11/07/2003. EE.UU. http://www.uaipit.com/files/documentos/pdf/0000004253_*SPAM*%20Act.pdf

- (2001). Anteproyecto de Ley de Delitos Informáticos. 21/11/2001. Argentina. http://www.uaipit.com/files/documentos/pdf/0000004491_ANTEPROYECTO%20DE%20LEY%20DE%20DELITOS%20INFORMATICOS.pdf

- (2003). Confidencialidad en la Economía Digital. 23/02/2003. Francia. http://www.uaipit.com/files/documentos/pdf/0000004744_Confidence%20in%20the%20Digital%20Economy.pdf

- (2000). Ley de 28 de Noviembre de 2000 Relativa a los Delitos Informáticos. 28/11/2000. Bélgica. http://www.uaipit.com/multilingue/documentos.jsp?len=es

- Departament of Justice. Criminal Division. U.S.A. Special report on "*phishing*". http://www.usdoj.gov/criminal/fraud/*Phishing*.pdf

- Dirección General para el desarrollo de la sociedad de la Información. Secretaria de Estado de Telecomunicación y para la Sociedad de la Información. Ministerio de Industria, Turismo y Comercio. Borrador de anteproyecto de Ley de Impulso de la Sociedad de la Información. http://www.internautas.org/archivos/pdf/Anteproyecto_LISI_080906.pdf

- Gago Figueroas, E.; Ramos Rodríguez, J.; González González, E. Ley Orgánica de Protección de Datos. http://www.extrenet.info/LOPD_SSI.pdf

- Grupo de Delitos Telemáticos; Unidad Central Operativa; Guardia Civil. Legislación. https://www.gdt.guardiacivil.es/legislacion.php

- Huerta, A.V. (2004). Códigos de buenas practicas de seguridad UNE-ISO/ IEC 17799. Grupo S2. 30/09/2004. Valencia. http://andercheran.upv.es/~toni/personal/ISO17799.pdf

- Javato Martin, A.M. (2005). La tutela penal del consumidor en el comercio electrónico en el derecho suizo. Revista electrónica de ciencia penal y criminología. 30/06/2005. http://criminet.ugr.es/recpc/07/recpc07-r2.pdf

Proveedores de seguridad

- *Malware* y *Phishing*, ¿ponemos más puertas al campo?. Ontinet.com, S.L. Nod32-es.com. http://www.nod32-es.com/news/documentos/*malware*_y_*phishing*.htm

- (2006). websense web Security Suite. http://www.afina.es/productos/websense/pdf/websense_webSecuritySuite.pdf

- Avira. (2006). ¿Qué es el *phishing*?. http://original.avira.com/es/paginas/que_es_el_*phishing*.html

- De la Cuadra, F. (2005). *Pharming*, nueva técnica de fraude. Panda Software. Marzo, 2005. http://www.pandasoftware.es/NR/rdonlyres/91E4A447-F6A1-4874-8AAA-2C2D262C9633/0/*Pharming*_spa_010305.pdf

- Departamento de Comunicación. Fraude en Internet: del *Phishing* al *Pharming*. Recovery Labs. Laboratorio de recuperación de datos informáticos. http://www.recoverylabs.com/informes/Recovery_Labs_*pharming*.pdf

- Fernández-Sanguino Peña, F.; Requejo Novella, A. (2005). Efectividad real de las estrategias contra el '*phishing*'. Germinus XXI, S.A. SIC, nº63. Febrero, 2005. http://www.germinus.com/sala_prensa/articulos/Efectividad%20real%20estrategias%20contra%20*phishing*.pdf

- Honeynet, G. (2005). Know your Enemy: *Phishing*. 16/05/2005. http://www.honeynet.org/papers/*phishing*/

- López, M. (2005). eToken: Bank Online Seguro. Channel Manager. Aladdin Knowledge Systems (NASDAQ: ALDN). http://www.ajoomal.com/descargas/aladdin/etoken/eToken%20value%20for%20on-line%20Banking%20-%20Esp.ppt

- McAfee Research – McAfee, Inc. (2005). McAfee Virtual Criminology Report: North American Study into Organized Crime and the Internet. – July 2005. http://www.mcafee.com/us/threat_center/white_paper.html

- McAfee Research – McAfee, Inc. (2006). Análisis de amenazas globales. http://inteco.red.es/observatorio/estudios.html

- McAfee Research – McAfee, Inc. (2006). McAfee Virtual Criminology Report: Organized Crime and the Internet. – December 2006. http://www.mcafee.com/us/threat_center/white_paper.html

- MessageLabs. (2006). MessageLabs Intelligence: 2006 Annual Security Report. http://www.messagelabs.com/Threat_Watch/Intelligence_Reports

- MessageLabs. (2007). MessageLabs Intelligence: Monthly Reports. http://www.messagelabs.com/Threat_Watch/Intelligence_Reports

- Mitxelena, X.; Gallo, M. (2006). Informe sobre fraude on-line 2005: estadisticas y recomendaciones para la lucha contra el *phishing* y otros ciberdelitos. S21sec. http://www.asimelec.es/htmventa/Noticias/redinoti/noticias/doc/Informe%20sobre%20Fraude%20On-line%202005%20-%20S21sec.pdf

- Nextira one México. Preguntas frecuentes de seguridad. http://www.nextiraone.com.mx/Datasheet/Preguntas_Frecuentes_Seguridad.pdf

- NGSSoftware Insight Security Research. (2004). The *Phishing* Guide. Understanding & Preventing *Phishing* Attacks. http://www.nextgenss.com/papers/NISR-WP-*Phishing*.pdf

- Ollman, G. (2004). The *Phishing* Guide. NISR Next Generation Security Software Ltd. Septiembre, 2004. http://www.ngssoftware.com/papers/NISR-WP-*Phishing*.pdf

- Pablo A. Silberpich. (2006). Análisis de normas y metodología que afectan a la gestión de la seguridad de la información. http://www.segurinfo.org.ar/old/06/presentaciones/b1000.pdf

- Pandasoftware. (2006). Informe trimestral Pandalabs. Abril-Junio, 2006. http://www.pandasoftware.es/NR/rdonlyres/0C542B09-0901-4D2A-9617-302453B385BA/0/InformeanualPandaLabs2005.pdf

- Recovery Labs. Laboratorio de recuperación de datos informáticos. *Phishing*: Fraude en Internet. http://www.recoverylabs.com/informes/Recovery_Labs_*phishing*.pdf

- Robledo, J.; Orellana, M. (2005). IpsCA blinda la seguridad de las operaciones on-line a través de sus dispositivos token. IpsCA. 22/04/2005. Madrid. http://www.ipsca.com/es/company/notasprensa/2005_04_22ipsCA%20blinda%20%20la%20seguridad%20de%20las%20operacion

- Ropero, R. (2004). Estudio sobre debilidades de diseño en páginas web de bancos on-line que favorecen ataques de *phishing*. Hispasec Sistemas. 16/11/2004.

http://www.hispasec.com/directorio/laboratorio/articulos/EstudioBanca*Phishing*/estudio_banca_y_*phishing*.pdf

- RSA. (2006). RSA monthly online fraud intelligence report.
- Sbampato, I.M. (2005). Amenazas contra el aparato financiero. Eset. http://www.nod32-a.com/documentos/amenazas.finan-01.pdf .
- Secure Computing, Inc. (2006). CipherTrust Proves Worldwide *Phishing* Attacks Originate from Fewer Than Five Zombie Network Operators. http://www.ciphertrust.com/resources/statistics
- Symantec. (2006). *Phishing* Attacks In and Around - April through September 2006. http://www.symantec.com/avcenter/reference/*phishing*-stats.pdf
- Symantec. (2007). Symantec Internet Security Threat Report (Volumes I-X). http://www.symantec.com/enterprise/threatreport/index.jsp
- Tally, G.; Thomas, R.; Van Vleck, T. (2004). Anti-*Phishing*: Best Practices for Institutions and Consumers. McAfee Research – McAfee, Inc. Informe Técnico N.º 04-004. Septiembre, 2004. http://www.governmentsecurity.org/articles/articles2/wp_anti_*phishing*.pdf_fl/
- Telefónica Empresas. Las TI en el sector bancario. Telefónica. El sector asegurador español. Whitepaper. http://www.empresas.telefonica.es/documentacion/WP_Banca.pdf
- Trend Micro. (2005). The trend of threats today: 2005 Annual Roundup and 2006 Forecast. http://www.trendmicro.com/en/security/white-papers/overview.htm
- Trend Micro. (2006). 2006 Annual Threat Roundup and 2007 Forecast. http://www.trendmicro.com/en/security/white-papers/overview/Threat_Roundup_Forecast.htm
- Tricipher. (2005). Zero-Footprint Solution to Combat *Phishing*. Whitepaper. Septiembre, 2005. http://www.anti-*phishing*.org/sponsors_technical_papers/tricipher-wp-zerofootprint.pdf
- Vázquez, J. *Phishing*, la estafa en la Red. Tb-Security. http://www.tb-security.com/articles/*phishing*.pdf
- Velasco López Urda, J.M. (2006). Evolucion de los servicios *anti-phishing* y de seguridad en Red: caso practico Grupo Popular. Servicios de seguridad desde la RED- Seguridad Gestionada. Telefónica Empresas. Abril, 2006.

http://proview.implanta.telefonicadata.com/.../Presentación%20*Phishing*%20Securmatica%202006%20v3.pdf

- Verisign Spain, S.L. (2005). Solución anti-*phishing* de Verisign. http://www.verisign.es/static/030190.pdf

- Verisign y Certisur. Vulnerabilidad de *phishing* en sitios bancarios en Argentina. http://www.certisur.com/docs/200508-*Phishing*_Bancos_Argentina.pdf

- Verisign. (2007). Internet Security Intelligence Briefing (diversos informes). http://www.verisign.com/Resources/Security_Services_White_Papers/Internet_security_briefing.html

- websense Security Labs. (2007). Security Trends Report (varios informes). http://www.websense.com/welcome/SecurityTrendReport/

Proveedores de servicios

- Arevacos. (2006). La asociación de internautas alerta sobre ofertas de trabajo fraudulentas para blanquear dinero del *phishing*. Jazztelia. 11/04/2006. http://www.jazztelia.com/arevacos/post/2006/04/11/la-asociacion-internautas-alerta-sobre-ofertas-trabajo

- Banco Santander. Seguridad. http://www.gruposantander.es/

- Microsoft Corporation. Todo lo que debe saber acerca del "*phishing*". http://www.microsoft.com/latam/seguridad/hogar/*spam*/*phishing*.mspx

- Paypal. Consejos de Seguridad y Prevencion de Fraude. http://www.paypal.com/es/cgi-bin/webscr?cmd=p/gen/fraud-prevention-outside

- Ponce, P. Seguridad de la información. SantaFe Associates Internacional. http://www.imaginar.org/iicd/tus_archivos/TUS5/introduccion.pdf

- Santos Pascual, E. (2006). El *SCAM* nuevo fraude informático. Microsoft. http://www.microsoft.com/spain/empresas/asesoria/*scam*.mspx

- Unysis. (2005). Identity theft prevention and detection: Are your branch banking customers at risk?. http://www.unisys.com

Noticias en los medios

- (2006). Ranking de Eset: el Stration sobrepasó al *phishing*. FuerteventuraDigital. 02/11/2006. http://www.fuerteventuradigital.com/noticias/Otros/2006/11/02/221949.asp

- (2006). Surge una nueva iniciativa basada en el voluntariado para combatir el *malware*. CIO España. 06/11/2006. http://www.idg.es/CIO/mostrarNoticia.asp?id=85544880&seccion=seguridad

- (2006). El *phishing* ha aumentado un 45% como consecuencia de la propagación de volksbanken. Informativos. 08/11/2006. http://informativos.net/Noticia.aspx?noticia=47451

- (2006). Tres detenidos por estafar mediante '*phishing*' más 21.000 euros. Terra Actualidad. 10/11/2006. http://actualidad.terra.es/nacional/articulo/detenidos_estafar_*phishing*_euros_1201086.htm

- (2006). Alertan por recrudecimiento del '*phishing*'. DiarioPyme. 13/11/2006. http://www.diariopyme.cl/newtenberg/1878/article-75149.html

- (2006). Según reporte de IronPort más del 50 por ciento de los ordenadores personales corporativos tienen algún tipo de virus. Infononews. 13/11/2006. http://www.infonos.com/ecm.php?Param=W0gMwAKxN&IdItem=3511

- (2006). Detectan correo para coaccionar el voto en EU. La crónica de Hoy. 14/11/2006. http://www.cronica.com.mx/nota.php?id_nota=271151

- (2006). PandaLabs detecta una operación que utiliza a los niños como reclamo. Árbol de Noticias. 18/11/2006. http://www.arboldenoticias.com/index.php?option=com_content&task=view&id=620&Itemid=44

- (2006). Tras el '*Phishing*' las cuentas bancarias vuelven a estar en peligro por el '*Vishing*' y el '*Smishing*'. DomoticaViva.com. IBLNews. 18/11/2006. http://www.domoticaviva.com/PHP/newsphp.php?id=708

- (2006). Colegio de Contadores advierte sobre estafas electrónicas vía email. Emol. 20/11/2006. http://www.economiaynegocios.cl/noticias/noticias.asp?id=96686

- (2006). Detenidas dos personas en Barcelona por su presunta implicación en una red de '*phishing*'. La Vanguardia. 22/11/2006. http://www.lavanguardia.es/gen/20061122/51293375124/noticias/detenidas-dos-personas-en-barcelona-por-su-presunta-implicacion-en-una-red-de-*phishing*-mossos-Internet-valladolid-rusia-ucrania.html

- (2006). El *phishing* encierra una red de crimen organizado. PC World Mexico. 22/11/2006. http://www.pcworld.com.mx/pcw_completo_noticias.asp?pcwid=2403

- (2006). Microsoft colabora con las autoridades en el combate contra el *phishing*". Consumer Eroski. 23/11/2006. http://www.consumer.es/web/es/tecnologia/2006/11/23/157573.php

- (2006). El '*phishing*' provoca unas pérdidas de 2.200 millones en EE UU. Cincodias. 24/11/2006. Madrid. http://www.cincodias.com/articulo/empresas/*phishing*/provoca/perdidas/200/millones/EE/UU/cdssec/20061124cdscdiemp_33/Tes/

- (2006). Llega el *phishing* a los móviles. Noticiasdot. 25/11/2006. http://www2.noticiasdot.com/publicaciones/2006/1106/2511/noticias251106/noticias251106-439.htm

- (2006). La Asociación de Internautas advierte sobre el robo de claves de correo electrónico en fechas navideñas. Libertad Digital. 27/11/2006. http://www.libertaddigital.com/noticias/noticia_1276293569.html

- (2006). España es el tercer objetivo mundial del *phishing*, según RSA. CIO España. 28/11/2006. http://www.idg.es/CIO/mostrarNoticia.asp?id=86371880&seccion=seguridad

- (2006). Symantec inaugura la Red de Denuncias de Estafas Electrónicas. Datafull. 28/11/2006. http://www.datafull.com/noticias/index.php?id=10064

- (2006). Numerosos pontevedreses se ven afectados por la oleada de ofertas de trabajo falsas por e-mail. La Voz de Galicia. 31/10/2006. http://www.lavozdegalicia.es/ed_pontevedra/noticia.jsp?CAT=112&TEXTO=5240859

- Abad, C. (2005). The economy of *phishing*: A survey of the operations of the *phishing* market. First Monday. Volumen 10, numero 9. 01/09/2005. http://www.firstmonday.org/issues/issue10_9/abad/

- Abogados Portaley. (2006). *Phishing*: Un peligro para la banca on-line. Delitos informaticos. 27/11/2006. http://www.delitosinformaticos.com/11/2006/delitos/fraudes/*phishing*-un-peligro-para-la-banca-on-line

- Barroso, D. Internet es como la conducción: es seguro si se toman precauciones. El Correo Digital. http://www.elcorreodigital.com/vizcaya/prensa/20061109/otros/Internet-como-conduccion-seguro_20061109.html

- Bedia, A. Estafa por email con la que consiguen tus datos bancarios: ¡Ojo al timo del *Phishing*!. Terra.

http://www.unionradio.com/img/descargas/Entendiendo%20las%20nuevas%20tecnolog%C3%ADas%20QUE%20ES%20EL%20*PHISHING*.doc

- Equipo Telecommunity. (2006). Firefox e Internet Explorer compiten por el trono anti-*phishing*. Telecommmunity. 23/11/2006. http://www.telcommunity.com/visor.php?id_noticia=18935

- Ercoreca, E.G. (2006). La mitad de los medios de pago de Europa ya tiene chip. Cincodias. 10/11/2006. http://www.cincodias.com/articulo/empresas/mitad/medios/pago/Europa/tiene/chip/cdssec/20061110cdscdiemp_31/Tes/

- Molist, M. (2006). La ciberdelincuencia se traslada a la 'web': Los ataques a través de HTTP y HTTPS aumentan con crecimientos del 90% respecto al año pasado. El País. 21/09/2006. http://www.elpais.com/articulo/red/ciberdelincuencia/traslada/web/elpportec/20060921elpcibenr_1/Tes/

- Pulido, F.J. (2006). Microsoft emprende una cruzada contra el *phishing* en Europa. PC World Digital. 23/11/2006. http://www.idg.es/pcworld/index.asp?link=estructura%2FVersionImprimir%2Easp&id=86244522

Fondo bibliográfico

- Aceituno Canal, V. (2004). Seguridad de la información. Creaciones Copyright. Las Rozas (Madrid)

- Álvarez Marañón, G.; Pérez García, P.P. (2004). Seguridad informática para empresas y particulares. McGraw-Hill Interamericana de España. Madrid.

- de Marcelo Rodao, J. (2003). Piratas cibernéticos: cyberwars, seguridad informática e Internet. RA-MA. Madrid.

- Doral, A. (2002). Seguridad en Internet y medios de pago electrónicos. Prentice may.

- Elledge, A. (2004). *Phishing*: An Analysis of a Growing Problem. SANS Institute.

- Emigh, A. (2005). Online Identity Theft: *Phishing* Technology, Chokepoints and Countermeasures. http://www.*anti-phishing*.org/*Phishing*-dhs-Report.pdf

- Emigh, A. (2006). The *Crimeware* Landscape: *Malware*, *Phishing*, Identity Theft and Beyond. http://www.*anti-phishing*.org/reports/APWG_*Crimeware*Report.pdf

- European Symposium on Research in Computer Security 11º. (2006). Computer security: ESORICS 2006 11th European Symposium on Research in Computer Security, Hamburg, Germany, September 18-20, 2006. Proceedings. Hamburg (Germany).
- Garfinkel,S.; Spafford, G. (1999). Seguridad y comercio en el web. McGraw-Hill. Madrid.
- González Rodríguez, M.; González Martel, C.; Suárez Araujo, C.P. (2003). Seguridad en la información: el problema de la distribución de claves II Congreso Internacional Sociedad de la Información y del Conocimiento. CISIC. Universidad Pontificia de Salamanca, Campus de Madrid. McGraw-Hill. Madrid.
- González, G. (1990). El libro de los virus y la seguridad informática. RA-MA.
- Gutiérrez Gallardo, J.D. (2005). Seguridad digital y *hackers*. Anaya Multimedia.
- International Conference on Detection of Intrusions and *Malware* and Vulnerability Assessment 3ª. (2006). Detection of Intrusions and *Malware*, and Vulnerability Assessment Third International Conference, DIMVA 2006, Berlin, Germany, July 13-14, 2006. Proceedings. Berlin (Germany).
- International Workshop on Security Protocols 11º. (2003). Security Protocols 11th International Workshop, Cambridge, UK, April 2-4, 2003, Revised Selected Papers. Cambridge (UK).
- Jakobsson, M.; Myers, S. (2007). *Phishing* and Countermeasures: Understanding the Increasing Problem of Electronic Identity Theft. John Wiley & Sons.
- James, L. (2005). *Phishing* exposed. Syngress Publishing, Rockland.
- Maiwald, E. (2005). Fundamentos de seguridad de redes. McGraw-Hill Interamericana.
- Mallery, J.; [et al.]. (2005). Blindaje de redes: tu red invulnerable a los *hackers*. Anaya Multimedia. Madrid.
- McNab, C. (2004). Seguridad de redes. Anaya Multimedia. Madrid.
- Northcutt, S.; Novak, J. (2001). Guía avanzada, detección de intrusos. Prentice Hall. Madrid.
- Sullivan, D. (2006). The Definitive Guide to Controlling *Malware*, Spyware, *Phishing*, and *Spam*. RealTime Publishers.
- Zemánek, J. (2004). Cracking sin secretos: ataque y defensa de software. RA-MA. Madrid.

ÍNDICE DE GRÁFICOS

ÍNDICE DE TABLAS

Instituto Nacional
de Tecnologías
de la Comunicación

www.inteco.es